COLLECTION GUIDE D'APPLICATION

PRISE EN COMPTE DE L'ENVIRONNEMENT INFORMATIQUE ET INCIDENCE SUR LA DÉMARCHE D'AUDIT

CNCC
COMPAGNIE NATIONALE DES COMMISSAIRES AUX COMPTES
EDITION

AVRIL 2003

8, RUE DE L'AMIRAL-DE-COLIGNY - 75001 PARIS
TÉLÉPHONE : 01 40 15 04 96 - TÉLÉCOPIE : 01 44 77 82 27
SITE INTERNET : http://www.cncc.fr
SITE EXTRANET : http://www.crcc.com.fr
EMAIL : cncc.edition@cncc.fr

SOMMAIRE

REMERCIEMENTS

Cet ouvrage a été élaboré sous l'égide de la Commission informatique de la CNCC (Président : Stéphane Lipski), en collaboration avec l'AFAI (Association française de l'audit et du conseil informatiques), par un groupe de travail regroupant des commissaires aux comptes, des experts en audit des systèmes d'information, des membres du service technique de la CNCC et composé des personnes suivantes :

- **Groupe de rédacteurs**
  - Emmanuel Gineste
  - Laurent Gobbi
  - Zouheir Guedri
  - Cécile Huet
  - Vincent Manière
  - Beatrice Pajczer
  - Vincent Péquignot
  - Gérard Pomper
  - Michel Richard
  - Renaud Ronchieri

- **Groupe de relecteurs**
  - Jean-Luc Barlet
  - Fabien Cleuet
  - Brigitte Guillebert
  - Jean-Paul Lamy
  - Jean-Michel Mathieu
  - Gilles Mercier
  - Eric Piou
  - Dominique Raynot
  - Xavier Rondeau
  - Isabelle Tracq-Sengeissen
  - Serge Yablonsky
  - Guy Zerah

Emmanuel Layot, conseiller technique de la Compagnie nationale des commissaires aux comptes, a assuré la coordination des études et de la rédaction.

INTRODUCTION

1. LES NORMES PROFESSIONNELLES

Le Conseil national des commissaires aux comptes a entériné courant 2000, la transposition dans le référentiel français des normes d'audit internationales de l'IFAC.

Cette transposition s'inscrit dans une démarche volontariste, engagée par la Compagnie nationale des commissaires aux comptes depuis plus de vingt ans, qui se fonde sur la poursuite des objectifs qui lui sont confiés par le décret d'août 1969 organisant la profession de commissaire aux comptes, à savoir : assurer le bon exercice de la profession en utilisant les meilleures pratiques.

Deux objectifs ont été fixés pour la réalisation des travaux de transposition :
- positionner clairement la France au regard du référentiel normatif international (IAASB),
- témoigner du haut degré de qualité de la certification des commissaires aux comptes.

Les normes professionnelles, intégrées dans le Recueil « Normes professionnelles et Code de déontologie » paru en décembre 2000 et mis à jour en juillet 2002, sont applicables pour l'audit des comptes des exercices ouverts à compter du 1er janvier 2001.

Le Recueil est divisé en huit sections :
- Introduction
- Dispositions relatives à l'exercice des missions
- Mission d'audit
- Mission d'examen limité
- Interventions définies par convention
- Vérifications et informations spécifiques
- Interventions définies par la loi ou le règlement
- Missions particulières confiées à un commissaire aux comptes

Parmi les normes relatives à la mission d'audit, celles qui traitent de « l'appréciation du contrôle interne » sont au nombre de trois :
- évaluation du risque et contrôle interne (norme CNCC 2-301),
- audit réalisé dans un environnement informatique (norme CNCC 2-302),
- facteurs à considérer lorsque l'entité fait appel à un service bureau (norme CNCC 2-303).

2. LES OBJECTIFS DU GUIDE

L'audit réalisé dans un environnement informatique peut poser au commissaire aux comptes des difficultés de mise en œuvre en termes d'approche, de nature des contrôles à réaliser et d'exploitation des résultats obtenus à l'issue de ces contrôles.

Toutefois, la prise en compte de l'environnement informatique lors de l'audit des comptes ne doit pas être confondue avec l'audit informatique d'un système d'information confié généralement à des experts spécialisés.

La Note d'information CNCC n° 25 intitulée « La démarche du commissaire aux comptes en milieu informatisé » publiée en 1995, avait déjà sensibilisé les professionnels sur ces difficultés.

L'émergence des nouvelles technologies de l'information ainsi que la complexité croissante des systèmes d'information automatisés a conduit la CNCC à élaborer le présent guide destiné

essentiellement à remplacer la précédente « Note d'information » et à privilégier les aspects opérationnels.

Il traite notamment :

- des apports de la norme CNCC 2-302 précitée,
- des domaines sensibles de la démarche du commissaire aux comptes en milieu informatisé.

Il intègre :

- une méthodologie de la prise en compte de l'environnement informatique dans la mission du commissaire aux comptes,
- des exemples pratiques portant sur la nature et l'étendue des travaux à mettre en œuvre,
- des outils opérationnels pour la mise en œuvre de techniques d'audit assistées par ordinateur.

3. L'APPROCHE METHODOLOGIQUE ET PEDAGOGIQUE

L'objectif principal du guide est de préciser et commenter les modalités d'application décrites dans la norme CNCC 2-302 et d'apporter au commissaire aux comptes des solutions opérationnelles ; il sera fait référence à ce texte pour aborder chaque étape de la démarche.

L'approche méthodologique retenue a en conséquence privilégié les spécificités de la démarche dans un environnement informatique, notamment en ce qui concerne :

- l'orientation et la planification de la mission (prise de connaissance),
- l'évaluation du risque inhérent et du risque lié au contrôle,
- la conception et l'exécution des tests de procédures et des contrôles substantifs.

4. LES APPORTS DE LA NORME CNCC 2-302 : « AUDIT REALISE DANS UN ENVIRONNEMENT INFORMATIQUE »

La norme CNCC 2-302 rappelle les principes fondamentaux suivants :

- l'existence d'un environnement informatique ne modifie pas l'objectif et l'étendue de la mission du commissaire aux comptes,
- l'utilisation d'un ordinateur modifie la saisie et le processus de traitement et de conservation des données et en conséquence peut avoir une incidence sur les systèmes comptable et de contrôle interne de l'entité,
- un environnement informatique peut ainsi avoir une incidence sur la démarche du commissaire aux comptes lors de :
  - la prise de connaissance des systèmes comptable et de contrôle interne,
  - la prise en compte du risque inhérent et du risque lié au contrôle,
  - la mise en œuvre des procédures d'audit.

La nature des risques dans un environnement informatique est liée aux spécificités suivantes :

- le manque de trace matérielle justifiant les opérations qui entraîne un risque plus important de non détection des erreurs contenues dans les programmes d'application ou les logiciels d'exploitation,
- l'uniformité du traitement des opérations qui permet d'éliminer quasiment toutes les erreurs humaines ; en revanche, les erreurs de programmation peuvent entraîner un traitement incorrect de toutes les opérations,
- la séparation insuffisante des tâches qui résultent souvent de la centralisation des contrôles,
- le risque d'erreurs et d'irrégularités qui peut provenir :

- d'erreurs humaines dans la conception, la maintenance et la mise en œuvre, plus importantes que dans un système manuel,
- d'utilisateurs non autorisés qui accèdent, modifient, suppriment des données sans trace visible.

Par ailleurs, la possibilité de détection de ces erreurs et irrégularités est affectée par le fait qu'elles sont souvent intégrées lors de la conception ou de la modification de programmes d'application ou de logiciels d'exploitation, et sont aussi difficilement identifiables dans le temps.

En résumé, les risques en milieu informatisé peuvent résulter de défaillances dans les activités informatiques générales, telles que :

- le développement et la maintenance des programmes,
- l'exploitation du système,
- les traitements particuliers,
- la sécurité physique,
- les contrôles d'accès pour les utilisateurs privilégiés.

La norme CNCC 2-302 met l'accent sur certaines spécificités à prendre en considération par le commissaire aux comptes pour atteindre l'objectif de l'audit. Ces spécificités concernent essentiellement :

- les compétences du commissaire aux comptes et de son équipe au regard de la complexité de l'environnement informatique de l'entité,
- la planification des aspects de l'audit susceptibles d'être influencés par l'environnement informatique de l'entité, en particulier l'importance des différentes assertions sous-tendant l'établissement des comptes affectés par le traitement informatisé d'une application comptable complexe notamment,
- l'appréciation du risque inhérent et du risque lié au contrôle dans un environnement informatique utilisant des systèmes importants et complexes,
- l'utilisation par le commissaire aux comptes de techniques d'audit assistées par ordinateur.

En ce qui concerne les compétences, la norme précise que le commissaire aux comptes « détermine si des compétences informatiques particulières sont nécessaires pour réaliser la mission ».

Si tel est le cas, il se fait assister par un professionnel possédant ces compétences qui peut être un collaborateur ou un spécialiste externe.

Le commissaire aux comptes applique dans ce cas la norme CNCC 2-503 « Utilisation des travaux d'un expert » pour justifier de l'adéquation de ces travaux avec l'objectif de l'audit.

5. RAPPEL DE LA NOTION DE RISQUE D'AUDIT

La norme CNCC 2-301 contient les définitions suivantes :

- le « risque d'audit » est le risque que le commissaire aux comptes exprime une opinion incorrecte du fait d'anomalies significatives contenues dans les comptes et non détectées. Il se subdivise en trois composants : le risque inhérent, le risque lié au contrôle et le risque de non détection,

- le « risque inhérent » est la possibilité que le solde d'un compte ou qu'une catégorie d'opérations comporte des anomalies significatives isolées ou cumulées avec des anomalies dans d'autres soldes ou catégories d'opérations, nonobstant les contrôles internes existants,

- le « risque lié au contrôle » est le risque qu'une anomalie dans un solde de compte ou dans une catégorie d'opérations, prise isolément ou cumulée avec des anomalies dans d'autres soldes de comptes ou d'autres catégories d'opérations, soit significative et ne soit ni prévenue, ni détectée par les systèmes comptable et de contrôle interne et donc non corrigée en temps voulu,

- le « risque de non détection » est le risque que les contrôles mis en œuvre par le commissaire aux comptes ne parviennent pas à détecter une anomalie dans un solde de compte ou dans une catégorie d'opérations qui, isolée ou cumulée avec des anomalies dans d'autres soldes de comptes ou d'autres catégories d'opérations, serait significative.

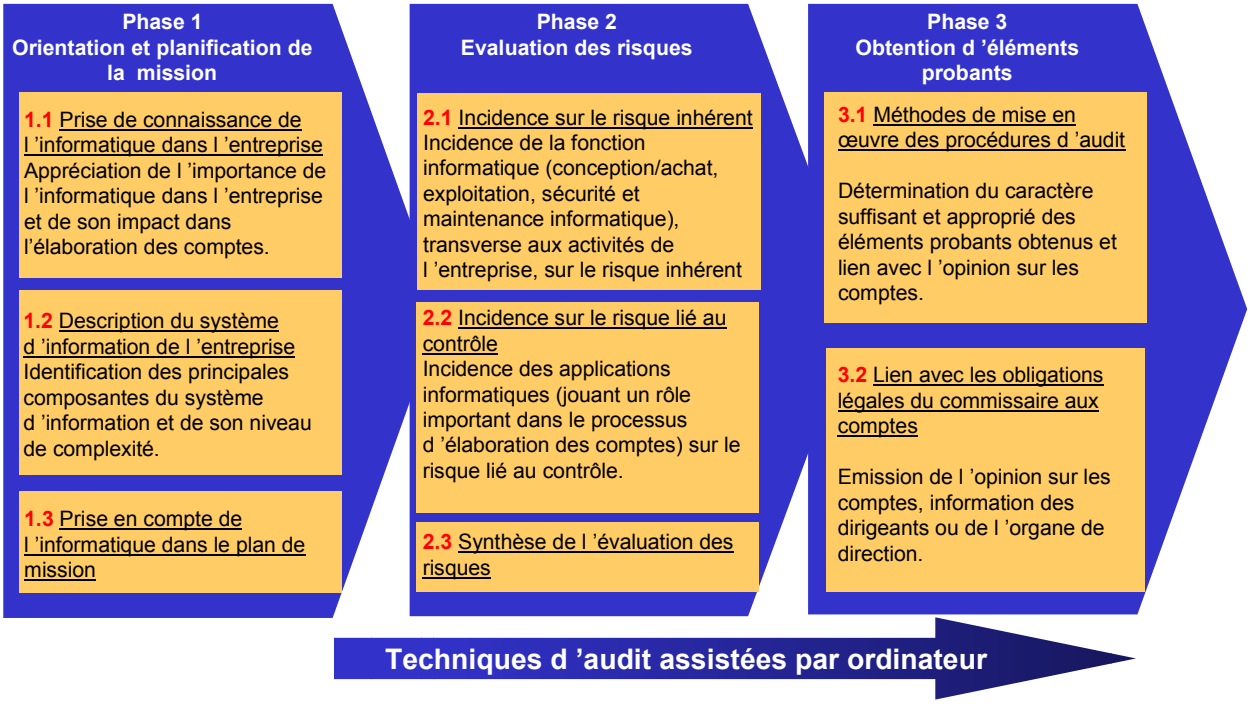
6. LA STRUCTURE DU GUIDE

Le guide comprend trois chapitres (la méthodologie, les dossiers thématiques, les techniques d'audit assistées par ordinateur) et des annexes (les supports opérationnels de mise en œuvre de la méthodologie, une étude de cas avec corrigé indicatif, un glossaire, un index et une bibliographie).

6.1. Méthodologie

Les spécificités de l'environnement informatique sont prises en compte dans les principales étapes de la démarche d'audit, à savoir :

- orientation et planification de la mission,
- évaluation des risques,
- obtention d'éléments probants.



6.2. Dossiers thématiques

Les dossiers thématiques développent des éléments théoriques et des concepts liés à des situations particulières. Ils sont volontairement exclus des développements consacrés à la méthodologie pour ne pas altérer leur caractère opérationnel. Les commissaires aux comptes peuvent utiliser ces dossiers thématiques de deux manières, soit pour se familiariser avec les systèmes d'information et maîtriser la signification de certains concepts ou de certains termes, soit pour approfondir un point particulier.

Les dossiers thématiques concernent les sujets suivants :

- l'organisation de la fonction informatique dans l'entreprise,
- les obligations réglementaires,
- les particularités en environnement PGI,
- les particularités en environnement Internet,
- les risques liés à l'existence d'un projet informatique.

6.3. Techniques d'audit assistées par ordinateur

Les techniques d'audit assistées par ordinateur peuvent être utilisées dans l'évaluation des risques et dans l'obtention d'éléments probants.

Elles utilisent des programmes d'interrogation de fichiers pour mettre en oeuvre des contrôles substantifs, comme par exemples :

- la vérification des calculs et additions (exemples : calcul des amortissements ; addition du fichier immobilisations ; calcul de la valeur des stocks et comparaison avec les états de gestion disponibles…),
- les comparaisons de fichiers et extractions d'anomalies (exemples : comparaison des fichiers des prix de revient et de vente de stocks pour identifier les dépréciations à effectuer ; extractions des stocks ou immobilisations dont la valeur nette est négative …),
- les extractions d'échantillons,
- le tri des fichiers selon des critères prédéfinis (exemples : ordre croissant des valeurs ; écritures passées sur une certaine période …).

6.4. Annexes

Les annexes comprennent notamment des supports opérationnels permettant la mise en œuvre de la méthodologie et une étude de cas illustrant la méthodologie de contrôle évoquée au chapitre 1.

6.4.1. Supports opérationnels

Le guide propose des supports opérationnels susceptibles d'aider le commissaire aux comptes dans les différentes étapes de la démarche d'audit.

6.4.2. Etude de cas

Une étude de cas, portant sur la prise en compte de l'environnement informatique dans une petite et moyenne entreprise, est proposée pour illustrer la mise en œuvre de la méthodologie. Les supports opérationnels présentés en annexe 1 sont utilisés pour traiter le cas.

Le corrigé de l'étude de cas est fourni à titre indicatif ; il ne peut être considéré comme un modèle.

CHAPITRE 1 : LA METHODOLOGIE

1. ORIENTATION ET PLANIFICATION DE LA MISSION

La phase « Orientation et planification de la mission » conduit à l'élaboration du plan de mission et implique la prise en compte du système d'information de l'entreprise.

Cette phase est particulièrement importante pour le bon déroulement de la mission ; elle représente souvent une part significative du budget d'heures, notamment la première année du mandat.

Pour les années suivantes, le poids relatif de cette phase par rapport à celle d'évaluation des risques et d'obtention des éléments probants pourra diminuer, sous réserve qu'aucune modification majeure n'intervienne dans l'environnement de l'entreprise et dans son organisation.

L'appréciation de l'incidence de l'environnement informatique nécessite :

- la prise de connaissance de l'informatique dans l'entreprise et de son incidence sur la production des informations financières et comptables,
- l'identification des principales composantes du système d'information et de son niveau de complexité.

1.1. Prise de connaissance de l'informatique dans l'entreprise

Elle consiste à collecter des informations sur les systèmes et les processus informatiques de l'entreprise et à en déduire leur incidence sur les procédures d'élaboration des comptes.

Les domaines à prendre en compte sont :

- la stratégie informatique,
- la fonction informatique de l'entreprise,
- l'importance de l'informatique dans l'entreprise.

1.1.1. La stratégie informatique

Objectif

La stratégie informatique de l'entreprise est à prendre en compte dans la définition du contenu du plan de mission.
Une position claire des dirigeants de l'entreprise quant à l'existant et aux évolutions futures du système d'information peut avoir une incidence sur l'évaluation des risques par le commissaire aux comptes. En revanche, la méconnaissance des risques auxquels l'entreprise est exposée au regard de l'utilisation de solutions informatiques et, plus généralement, des faiblesses constatées dans la maîtrise du système d'information, doivent conduire le commissaire aux comptes à une vigilance accrue et à mettre en place des contrôles plus importants.

Travaux à réaliser

Les éléments à considérer pour apprécier la stratégie informatique sont les suivants :

- implication des entités opérationnelles dans la détermination de la stratégie informatique :
  - perception de la place de l'informatique par les directions opérationnelles,
  - objectifs de l'informatique (réduire les coûts ou acquérir un avantage concurrentiel),
  - processus d'élaboration de la stratégie informatique (définition / validation),
- niveau de connaissance de la direction concernant le système d'information :
  - compréhension de l'exposition au risque,
  - mesures prises pour réduire les risques informatiques,
- satisfaction des besoins courants par le système d'information :
  - satisfaction des utilisateurs,
  - niveau d'erreurs (évolution des indicateurs qualité),
  - flexibilité des systèmes et capacité à évoluer (adaptation de l'informatique au métier et non l'inverse).

Modalités pratiques

Cette appréciation peut s'effectuer par :

- l'obtention de documents préalablement à l'intervention :
  - schéma directeur du système informatique et de la sécurité informatique,
  - budget informatique des trois dernières années et prévisions,
  - comptes-rendus de l'activité informatique des trois dernières années,
- l'entretien avec un représentant de la direction et l'obtention de documents complémentaires :
  - compréhension de la politique générale de l'entreprise, de ses enjeux actuels et futurs,
  - prise de connaissance du rôle que doit jouer l'entité ou la personne en charge des systèmes d'information dans le cadre de cette politique et de ses éventuelles difficultés,
  - compréhension des contrôles de l'activité informatique effectués par la direction,
  - faits majeurs à noter dans le domaine informatique et les domaines connexes (incidents importants : rupture de services/fraudes/malveillance),
- une confirmation des informations obtenues lors de l'entretien avec la direction :
  - étude des documents obtenus pendant l'entretien,
  - entretiens avec le responsable informatique,
- l'entretien avec des utilisateurs clés représentatifs des différentes entités opérationnelles,
- une communication des projets en cours ou prévus (part du budget informatique dans le budget total de la structure).

L'analyse de la stratégie informatique dans le plan de mission conduit à déterminer des situations où le risque sur la fiabilité du système d'information sera plus ou moins important.

	Incidence sur la fiabilité du système d'information		
	Faible	**Modérée**	**Elevée**
Stratégie informatique élaborée par les entités opérationnelles	La stratégie informatique existe (formalisée ou non). Les besoins utilisateurs sont pris en priorité pour élaborer la stratégie informatique.	Les besoins utilisateurs sont considérés dans la stratégie informatique.	La stratégie informatique n'est pas formalisée. Absence de coordination entre la stratégie informatique et la stratégie de l'entreprise.
Sensibilisation de la direction	La direction est sensibilisée à la valeur ajoutée de l'informatique.	La valeur de l'informatique et l'exposition aux risques sont connues par la direction. En revanche, cette connaissance par les niveaux hiérarchiques inférieurs est partielle.	La direction est consciente de la valeur et des risques de l'informatique alors que les entités opérationnelles ne le sont pas.
Satisfaction des besoins utilisateurs	Les besoins utilisateurs sont satisfaits par les technologies utilisées actuellement. La satisfaction des utilisateurs est mesurée périodiquement.	Les systèmes répondent globalement aux besoins. Quelques systèmes sont difficiles à maintenir.	La plupart des applications ne répond pas aux besoins des utilisateurs. Des travaux supplémentaires sont nécessaires pour combler les manques du système d'information.

Résultat

Les différents éléments à analyser sont relativement indépendants. Cependant, si la direction n'est pas sensibilisée à l'importance du système d'information et ne participe pas à l'élaboration de la stratégie informatique, il existe un risque potentiel d'inadéquation de l'outil informatique aux besoins des entités opérationnelles.

Les risques potentiels associés aux éléments visés ci-dessus sont :

- la non prise en compte d'investissements importants qui seront nécessaires pour adapter le système d'information aux besoins de l'entreprise (budget important lié aux projets de type PGI (Programme de Gestion Intégré) / ERP (Enterprise Resource Planning)),
- la non continuité d'exploitation liée à une mauvaise orientation de la stratégie informatique et à l'incapacité du système d'information à s'adapter aux évolutions de l'entreprise et des besoins de ses clients.

Exemple 1

Les utilisateurs sont fortement impliqués dans les choix informatiques majeurs. Des représentants des utilisateurs participent à la validation du plan informatique définissant les objectifs et l'emploi des ressources informatiques (calendrier général, budget).
Le responsable informatique est conscient des enjeux liés aux réglementations en vigueur et s'est fixé comme objectif principal la mise en conformité de ces activités.

➔ Incidence sur la fiabilité du système d'information : Faible

Exemple 2

Une société présentant une informatique vieillissante, développée par des informaticiens partis depuis lors à la retraite, ne peut plus adapter son système d'information à ses nouvelles contraintes. Si les programmes sont complexes et mal documentés, il est probable que plus personne ne sera en mesure de faire évoluer les systèmes d'information : il faudra donc les refondre totalement.
Si cette société souhaite orienter sa stratégie générale de façon à être plus proche de ses clients, en développant des interfaces entre son système d'information et Internet (exemple : saisie en ligne de commandes), les adaptations du système peuvent s'avérer très difficiles à mettre en œuvre ou très coûteuses.
Cette société risque d'avoir de grandes difficultés à atteindre sa stratégie client dans la mesure où son informatique est mal adaptée.

➔ Incidence sur la fiabilité du système d'information : Elevée

1.1.2. La fonction informatique

La fonction informatique de l'entreprise est à prendre en compte dans la définition du contenu du plan de mission, notamment en termes de séparation des fonctions, gestion des mouvements de personnel, gestion des projets, fiabilité des processus informatiques (pilotage, développement, maintenance, exploitation, sécurité du système d'information).

A. L'organisation de la fonction informatique

Objectif

L'étude de l'organisation de la fonction informatique consiste à considérer son adéquation aux besoins et aux enjeux de l'entreprise, le respect du principe de séparation des tâches et le niveau de dépendance de l'entreprise vis-à-vis de prestataires externes.

Travaux à réaliser

Les éléments utiles à l'étude de l'organisation de la fonction informatique sont les suivants :

- les caractéristiques de l'organisation informatique :
  - l'existence ou non de la fonction informatique,
  - la vérification de l'existence d'un organigramme à jour comprenant une définition des fonctions et un partage clair des rôles et des responsabilités pour chaque poste,
  - la vérification que l'ensemble des composantes d'une fonction informatique est convenablement pris en compte et notamment : exploitation, études, et sécurité informatique,
- la séparation des tâches :
  - le caractère distinct des tâches et des environnements relatifs aux fonctions Études et Exploitation,
  - le maintien de la séparation des tâches lors de la rotation des équipes, des congés ou du départ d'un salarié,
- le recours aux prestataires :
  - nombre de prestataires,
  - degré de dépendance vis-à-vis des prestataires,
  - fonctions exercées.

Modalités pratiques

Afin de réaliser cette étude, il est nécessaire d'organiser des entretiens avec le responsable informatique. Ces entretiens portent sur les sujets suivants :

- description de l'organigramme général et de la fonction informatique,
- description des postes, des fonctions et des responsabilités des membres de la fonction informatique,
- tâches effectuées par l'informatique et localisation géographique des services,
- recours à la sous-traitance,
- séparation des tâches.

Les informations recueillies auprès du responsable informatique peuvent être complétées en effectuant des entretiens avec les responsables des départements opérationnels.

L'analyse de l'organisation de la fonction informatique dans le plan de mission conduit à déterminer des situations où le risque sur la fiabilité du système d'information sera plus ou moins important.

	Incidence sur la fiabilité du système d'information		
	Faible	**Modérée**	**Elevée**
Organisation informatique	Fonctions gérées par des services indépendants. Fonction sécurité exercée par un responsable dédié. Organisation adaptée aux besoins. Représentation de la fonction informatique auprès de la direction. Informations concernant la gestion de l'informatique fournies à direction.	Fonction sécurité existant partiellement. Définition peu claire des rôles et responsabilités. Représentation non systématique de la fonction informatique auprès de la direction.	Services partageant plusieurs fonctions (notamment les études et l'exploitation). Fonction sécurité non gérée. Pas de représentation de la fonction informatique auprès de la direction. Rôles et responsabilités non définis de manière claire.
Séparation des tâches	Séparation assurée à tous les niveaux. Suivi de cette séparation. Implication des utilisateurs.	Séparation assurée mais aucun contrôle réalisé. Faible implication des utilisateurs.	Les mêmes personnes ont en charge les études et l'exploitation. Aucune implication des utilisateurs.
Externalisation *	Toutes les fonctions sont assurées par l'entreprise.	Quelques fonctions sont partiellement externalisées.	Fonctions sensibles externalisées. Ressources internes réduites.

* L'appréciation du risque entraîné par l'externalisation de la fonction informatique doit également porter sur l'analyse du contrat qui lie l'entreprise à son prestataire, ainsi que sur la maîtrise par l'entreprise des prestations sous-traitées.

Résultat

Les différents éléments sont totalement indépendants tout en se révélant d'un même niveau d'importance pour l'entreprise. Cela signifie que si l'un d'eux présente des faiblesses, alors l'organisation informatique dans son ensemble aura une incidence élevée sur les risques à évaluer.

Les risques potentiels liés à l'organisation de la fonction informatique peuvent se traduire de la façon suivante pour le commissaire aux comptes :

- l'absence de séparation des fonctions peut impliquer un plus grand risque de fraude,
- l'absence de maîtrise du système d'information (sous-traitants non encadrés, manque de compétences internes sur certains thèmes) peut impliquer un risque sur la continuité de l'exploitation,
- des erreurs de développement ou l'incapacité du département informatique à maintenir une application peuvent avoir pour conséquence des erreurs dans la valorisation des flux ou un risque de non exhaustivité des enregistrements comptables.

Exemple 1

L'organigramme du département informatique ne présente aucune séparation des fonctions entre les fonctions « Etudes » et « Exploitation ». En effet, le même service réalise les développements, les tests, la mise en production et l'exploitation des applications. D'autre part, le département informatique s'appuie sur de nombreux prestataires pour renforcer ses propres équipes. L'exploitation du Progiciel de Gestion Intégré supportant les principales opérations de l'entreprise est externalisée auprès d'un prestataire.

➔ Incidence sur la fiabilité du système d'information : Elevée

Exemple 2

L'entreprise X est une petite structure, il n'y a qu'un seul informaticien. Ce dernier a développé, il y a de nombreuses années, une application informatique de gestion des ventes relativement complexe. Ses travaux de développement n'ont pas été documentés et il est le seul à maintenir l'application. Il a par ailleurs accès à toutes les autres applications de l'entreprise (comptabilité, achats, …).

Il existe un risque en termes de continuité d'exploitation en cas de départ de cet informaticien. En effet, ses programmes n'étant pas documentés, la maintenance de l'application de gestion des ventes sera difficile à assurer. Cette dernière devra vraisemblablement être réécrite et reprise par une nouvelle personne dès qu'apparaîtra le besoin de la faire évoluer.

En outre, il existe un risque de fraude car l'informaticien est administrateur de toutes les applications informatiques (absence de séparation de fonctions). Le supérieur hiérarchique de l'informaticien devra s'assurer que l'informaticien ne modifie pas des données de production sans la supervision d'un responsable fonctionnel.

➔ Incidence sur la fiabilité du système d'information : Elevée

B. Les compétences informatiques

Objectif

L'étude des compétences informatiques consiste à considérer le niveau de compétence du personnel, la charge de travail, le niveau de rotation du personnel informatique de l'entreprise.

Travaux à réaliser

Les éléments à prendre en compte dans l'étude des compétences informatiques sont les suivants :

- niveau de compétence :
  - compétences en rapport avec les besoins actuels et futurs notamment dans la perspective programmée d'un changement de technologie,
  - niveau de formation,
  - mesure des performances du personnel,
- charge de travail par rapport aux ressources humaines disponibles :
  - niveau d'occupation (nombre heures supplémentaires/nombre heures travaillées),
  - importance de la dépendance vis-à-vis des personnes clés,
  - existence des ressources nécessaires pour l'exécution des opérations régulières (validation du responsable de service pour prise de congés, modalités de gestion des 35 heures),

- niveau de rotation du personnel :
  - nombre de départs sur les deux dernières années,
  - stabilité du niveau d'occupation,
  - motivation des collaborateurs.

Modalités pratiques

Cette étude peut s'effectuer :

- par entretiens avec le responsable informatique sur :
  - l'évolution du budget formation sur les trois dernières années,
  - les mesures de performances du personnel informatique,
  - le niveau d'occupation du personnel (nombre heures supplémentaires/nombre heures travaillées),
  - la dépendance vis-à-vis des personnes clés par l'étude de la répartition des heures supplémentaires,
  - l'évolution du taux d'occupation des collaborateurs (évolution des heures travaillées sur les 3 dernières années),
  - le degré de motivation des collaborateurs (prise de connaissance des comptes-rendus annuels d'entretien),
- par l'analyse des documents suivants :
  - calendrier des formations,
  - comptes-rendus annuels des entretiens d'évaluation,
  - rapprochement du calendrier des formations avec les comptes-rendus annuels,
- par des entretiens avec des utilisateurs clés représentatifs des différentes directions.

Afin de confirmer les informations collectées précédemment, il peut être nécessaire de rencontrer un collaborateur du département informatique. Les acteurs en charge de la sécurité technique, de l'administration du réseau, de la gestion des bases de données, peuvent nécessiter des compétences pointues.

L'analyse des compétences informatiques dans le plan de mission conduit à déterminer des situations où le risque sur la fiabilité du système d'information sera plus ou moins important.

	Incidence sur la fiabilité du système d'information		
	Faible	**Modérée**	**Elevée**
Niveau de compétence	Personnel qualifié et motivé à tous les niveaux de la hiérarchie. Programme de formation défini en accord avec la stratégie de l'entreprise pour l'acquisition de nouvelles compétences et la conservation du personnel.	Personnel inégalement qualifié et personnel nouvellement embauché. Budget de formation défini.	Personnel inexpérimenté et peu formé. Démotivation.
Charge de travail	Ressources humaines suffisantes pour couvrir les besoins actuels. Revue des ressources réalisée périodiquement pour s'assurer de	Ressources suffisantes pour les besoins actuels. Estimation informelle des futures charges de travail. Heures supplémentaires	Déficit en ressources. Pas de mesure des besoins. Dépendance vis-à-vis des personnes clés. Absence de budget pour augmenter les ressources.

	Incidence sur la fiabilité du système d'information		
	Faible	**Modérée**	**Elevée**
	l'adéquation avec les besoins.	régulièrement nécessaires.	
Niveau de rotation	Rotation limitée. Toutes les activités sont couvertes par des personnes expérimentées.	Rotation régulière. Mesures mises en place afin de remplacer les personnes clés dans des délais raisonnables	Rotation fréquente du personnel. Difficultés pour retenir le personnel. Difficultés à remplacer les personnes clés.

Résultat

La prise en considération individuelle des éléments cités précédemment permet d'apprécier globalement l'incidence que peuvent avoir les compétences informatiques sur le plan de mission.

Exemple

Le personnel en charge de l'exploitation informatique est stable malgré l'emploi de prestataires. La réorganisation induite par l'application des 35 heures implique une charge de travail importante. Le personnel demeure cependant motivé.
Le département informatique est constitué pour sa grande majorité de prestataires. Ceci, ajouté à l'actuelle rareté de profils adaptés sur le marché du travail, a pour conséquence une forte rotation du personnel.
Les compétences du personnel satisfont les besoins liés aux technologies utilisées. Elles sont régulièrement mises à jour au travers de formations.

➔ Incidence sur la fiabilité du système d'information : Modérée

1.1.3. Importance de l'informatique dans l'entreprise

Objectif

L'importance de l'informatique dans l'entreprise permet de déterminer le niveau de dépendance de l'entreprise vis-à-vis de son système d'information.

Travaux à réaliser

Les éléments à prendre en compte pour apprécier l'importance de l'informatique dans l'entreprise sont les suivants :

- degré d'incidence de l'informatique sur la production des informations comptables et financières,
- degré d'automatisation :
  - nombre de traitements automatisés,
  - taille des systèmes,
  - nombre d'opérations traitées,
  - organisation limitant l'utilisation du papier,
- caractéristiques du système d'information :
  - besoins de l'activité, volume de transactions important,
  - utilisation importante de technologies (EDI, Internet),
  - exploitation en temps réel ou traitement par lot différé,
  - génération automatique d'opérations,
- utilisation et sensibilité de l'informatique :
  - impact sur la production des comptes,
  - informations confidentielles stockées dans les systèmes,
  - contexte réglementaire important (CNIL, etc.),
  - utilisation des systèmes pour développer de nouveaux produits par rapport aux concurrents,
- temps d'indisponibilité maximale tolérable :
  - activité dépendante de l'informatique (nécessaire pour maintenir les revenus de l'entreprise),
  - impacts d'une interruption du système d'information (pertes opérationnelles, pertes financières, continuité d'exploitation).

Modalités pratiques

Afin de réaliser cette analyse, il est nécessaire d'organiser des entretiens avec la direction et le responsable informatique. Ces entretiens portent sur les sujets suivants :

- description du système d'information :
  - principales applications,
  - principaux traitements,
- importance des données et des traitements au regard de la continuité d'exploitation,
- estimation du temps d'indisponibilité du système et méthode employée pour l'estimer,
- dysfonctionnements notés durant l'année précédente (interruption de service, actes frauduleux, etc.).

Les informations recueillies peuvent être complétées en effectuant des entretiens auprès des responsables de domaines opérationnels ou d'utilisateurs clés. Ces entretiens permettent de mieux comprendre l'importance des données et des traitements dans le fonctionnement de l'entreprise, ainsi que les enjeux du métier par rapport au système d'information.

L'analyse de l'importance de l'informatique dans le plan de mission conduit à déterminer des situations où le risque sur la fiabilité du système d'information sera plus ou moins important.

	Incidence sur la fiabilité du système d'information		
	Faible	**Modérée**	**Elevée**
Degré d'automatisation	Peu de traitements automatisés – Informatique utilisée pour conserver des informations historiques. Les traitements différés sont lancés manuellement.	Beaucoup de traitements automatisés – Utilisation de la bureautique.	La majorité des tâches de l'entreprise est automatisée, fortement dépendante de l'informatique.
Caractéristiques du système d'information	Systèmes simples pour conserver des enregistrements et fonctionnant par des traitements différés.	Mélange de systèmes temps réel et de traitements différés. Générations de quelques opérations automatiquement	Systèmes temps réel générant de nombreuses opérations automatiquement. Utilisation de nouvelles technologies.
Sensibilité de l'informatique	Utilisation limitée de l'informatique – peu d'informations sensibles stockées dans les systèmes.	Informations importantes (données personnelles, détails des produits et services) conservées dans le système d'information.	Informations hautement sensibles et confidentielles gérées par le système. Nombreux contrôles nécessaires.
Indisponibilité	Informatique non nécessaire à l'activité de l'entreprise. Possibilité de revenir à une organisation uniquement basée sur le papier.	Entreprise dépendante de l'informatique – Traitements clés nécessaires pour maintenir les ressources de l'entreprise après une période d'interruption.	Entreprise hautement dépendante de l'informatique. Des pertes importantes, pouvant mettre en péril la survie de l'entreprise, pourraient survenir en cas d'indisponibilité supérieure à quelques heures.

Résultat

L'évaluation des différents éléments précédents permet d'obtenir une idée satisfaisante de l'importance de l'informatique de l'entreprise. Ces éléments sont liés les uns aux autres.
Si l'un d'entre eux a une incidence élevée sur les contrôles à effectuer, il existe alors des risques potentiels liés à la place de l'informatique dans l'entreprise.

Exemple

L'entreprise est fortement dépendante de son informatique. La majorité des opérations s'effectue au travers de systèmes informatiques complexes. Une interruption de service supérieure à 4 heures pourrait entraîner la rupture des traitements en temps réel, engendrant des pertes opérationnelles et financières importantes.

➔ Incidence sur la fiabilité du système d'information : Elevée

1.2. Description du système d'information de l'entreprise

La norme CNCC 2-302 précise dans le paragraphe .07 - que « dans un environnement informatique utilisant des systèmes importants et complexes, le commissaire aux comptes acquiert également la connaissance de cet environnement et détermine si celui-ci peut influencer l'évaluation du risque inhérent et l'évaluation du risque lié au contrôle ».

La description du système d'information de l'entreprise consiste à :
- formaliser la cartographie des applications,
- apprécier le degré de complexité du système d'information,
- identifier les processus à analyser, utiles aux objectifs de l'audit.

1.2.1. Cartographie générale des applications

Objectif

La réalisation d'une cartographie générale des applications permet de comprendre et de documenter les composantes du système d'information. Elle permet en outre de mettre en évidence les risques potentiels liés à cette architecture.

Travaux à réaliser

L'établissement de la cartographie du système d'information nécessite l'identification des principales applications et interfaces.

Identification des principales applications informatiques

L'identification des applications informatiques concerne le recensement des applications qui composent le système d'information de l'entreprise. Pour chacune d'elles, il est nécessaire de connaître :
- le type (progiciel avec indication de l'éditeur/développement spécifique),
- la date de mise en place,
- l'environnement technique : UNIX, Windows, AS400...,
- le mode de traitement (différé ou temps réel),
- le nom de l'éditeur ou du prestataire,
- la date de la dernière modification,
- les principales fonctionnalités,
- la nature des sorties,
- une estimation du volume traité.

Identification des principales interfaces

L'identification des principales interfaces concerne les liens qui existent entre les différentes applications. Ces liens peuvent être automatiques, semi-automatiques ou manuels. Pour chaque interface identifiée, il est nécessaire de connaître :
- le type d'interface : automatique, semi-automatique, manuel,
- les applications en amont / en aval,
- la nature des flux : ventes, stocks, clients…,
- la fréquence : quotidienne, hebdomadaire, mensuelle…,
- les états d'anomalies.

Résultat

La représentation graphique des différentes applications et des liens existant entre elles constitue la cartographie générale des applications. Elle permet de visualiser de façon synthétique un système d'information complexe et sert en outre de support de communication pluridisciplinaire (culture comptable, culture informatique) dans l'identification des risques potentiels.

Pour les systèmes très simples (2 à 3 applications), la cartographie pourra se limiter à la formalisation de tableaux d'inventaire établis par le commissaire aux comptes, alors que pour les systèmes d'information très complexes, l'intervention d'un expert informatique peut être nécessaire.

La cartographie des applications peut être complétée avec une description de l'infrastructure technique : matériels et réseaux.

Exemples

Des exemples de cartographies avec description de l'infrastructure technique sont disponibles dans l'Annexe 1 « Les supports opérationnels : description du système d'information de l'entreprise ».

1.2.2. Appréciation de la complexité du système d'information

Objectif

La complexité du système d'information est un élément important à prendre en compte lors de l'établissement du plan de mission.
Son appréciation permet de décider si des compétences informatiques particulières sont nécessaires pour réaliser la mission et s'il convient que le commissaire aux comptes se fasse assister d'un expert.

Travaux à réaliser

L'appréciation de la complexité du système d'information concerne l'ensemble des applications et s'effectue au travers de l'analyse de la cartographie en prenant en compte les critères suivants :

- existence de progiciel intégré ou de nombreuses applications spécifiques,
- technologie utilisée : système central, client serveur, Internet…,
- paramétrage : complexité, étendue, paramètres standards ou définis par l'entreprise,
- nombre d'interfaces,
- existence d'interfaces manuelles entre les systèmes,
- dépendance des traitements entre les systèmes.

Modalités pratiques

La complexité du système d'information de l'entreprise va pouvoir être appréciée à partir de la cartographie réalisée précédemment et de la documentation fournie (cette dernière n'a pas d'incidence sur la complexité du système, mais son existence et sa qualité permettent une analyse plus fine).

Cette étude peut être complétée par un entretien avec le responsable informatique pour couvrir les points suivants :

- existence ou non d'une documentation,
- degré de mise à jour de la documentation en fonction des évolutions du système d'information,

- dépendance des traitements entre les systèmes.

L'analyse de la complexité du système d'information dans le plan de mission conduit à déterminer des situations où le risque sur la fiabilité du système d'information sera plus ou moins important.

	Incidence sur la fiabilité du système d'information		
	Faible	**Modérée**	**Elevée**
Intégration	Système entièrement intégré utilisant des informations partagées entre les applications (existence de référentiels). Les fonctions d'états de synthèse et de tableaux de bord sont intégrées dans le système.	Quelques interfaces sont automatisées. Des informations sont traitées sur poste client à des fins d'états de synthèse et de tableaux de bord.	Système fragmenté nécessitant la saisie manuelle de nombreuses informations entre les systèmes. Données en doublons en raison de l'inexistence de référentiels. Pas de règle de gestion concernant la mise à jour des données.
Documentation	Existence d'une documentation à jour permettant d'avoir une bonne compréhension du système d'information.	Documentation partielle mais couvrant les principales applications.	Documentation faible ou non mise à jour. Difficulté à appréhender le système et à mesurer l'impact d'une modification.

Les risques potentiels liés aux systèmes fortement intégrés sont à nuancer avec les connaissances que le commissaire aux comptes aura acquises sur l'organisation informatique et les compétences du personnel informatique. En effet, bien qu'une telle architecture minimise les risques compte tenu de l'utilisation de bases de données homogènes et d'interfaces inter-modules, l'intégrité des informations est fortement soumise aux corrects paramétrage, administration et utilisation du système. Il conviendra donc de s'assurer que ces systèmes sont maîtrisés par le service informatique et les utilisateurs, avant de considérer que les résultats des traitements sont fiables.

Résultat

La prise en compte des éléments ci-dessus permet d'apprécier la complexité du système d'information. Dans le cas d'un système très complexe faisant appel aux nouvelles technologies, le commissaire aux comptes pourra faire appel à un expert afin d'identifier les zones de risques majeures.
Par la suite, l'expert pourra éventuellement apporter une assurance complémentaire sur :

- la fiabilité des informations gérées au travers du système d'information,
- le respect des procédures de contrôle interne sur les flux opérationnels.

Exemple

Le système d'information reflète le développement de l'entreprise, réalisé principalement par croissance externe. En effet, il est constitué d'un nombre important d'applications hétérogènes liées les unes aux autres par de nombreuses interfaces. Ces différentes applications se trouvent sur des plates-formes techniques différentes gérées par des équipes distinctes. La documentation de ces systèmes est partielle et de qualité inégale. Elle ne permet pas d'obtenir une vue synthétique des différents composants du système d'information.

➔ Incidence sur la fiabilité du système d'information : Elevée

1.2.3. Identification des processus à analyser

Objectif

L'évaluation des risques n'est pas seulement influencée par les seules applications informatiques. En effet, l'incidence de l'environnement informatique sur le risque inhérent et le risque lié au contrôle ne peut être appréciée sans prendre en compte la notion de flux d'information ou processus.

Un processus peut être défini comme « un enchaînement de tâches, manuelles, semi-automatiques, automatiques, concourant à l'élaboration, à la production ou au traitement d'informations, de produits ou de services. Exemples : processus de gestion des ventes, processus de gestion des impayés, processus de fabrication, processus d'inventaire permanent, processus d'établissement des comptes, etc.».

Le commissaire aux comptes ne s'intéresse pas à l'ensemble des processus existant au sein de l'entreprise, mais uniquement à ceux contribuant directement ou indirectement à la production des comptes. Les processus étudiés sont alors, dans la majorité des cas, les suivants : achats, ventes, stocks, règlements, paie.

Seules les applications (et leurs inter-relations) qui interviennent dans ces processus méritent de faire l'objet d'une étude dans le cadre de la démarche d'audit.

Travaux à réaliser

Pour chacun des processus concourant directement ou indirectement à la production des comptes, il est nécessaire de déterminer les applications qui participent aux traitements des données. Cette détermination s'effectue à partir de la cartographie réalisée précédemment.

Selon l'importance du rôle joué par les applications et les interfaces dans chaque processus, le commissaire aux comptes sélectionne le ou les processus à analyser dans le cadre de son évaluation des risques.

Ainsi, l'analyse d'une application peut nécessiter l'analyse de plusieurs processus, lorsqu'une même application intervient dans plusieurs processus.

Résultat

Le résultat peut être formalisé sous forme du tableau suivant :

	Appli. 1	Appli. 2	Appli. 3	Appli. 4	Appli. 5	Appli. 6	Appli. 7
Processus 1	✓	✓	✓		✓		✓
Processus 2		✓	✓		✓		
Processus 3		✓	✓			✓	

Si l'application 5 présente des risques potentiels importants compte tenu de son obsolescence, du nombre de fonctionnalités et de l'importance des données gérées, on peut conclure que les processus 1 et 2 devront faire l'objet d'une analyse approfondie afin de pouvoir réduire le risque d'audit à un niveau faible acceptable.

Exemple

Un exemple est fourni dans l'étude de cas en Annexe.

1.3. Prise en compte de l'informatique dans le plan de mission

La norme CNCC 2-201 « Planification de la mission » prévoit dans son paragraphe .08 - que « le commissaire aux comptes élabore un plan de mission décrivant l'approche générale des travaux d'audit et leur étendue. Il consigne dans ses dossiers de travail la justification des choix opérés lors de la préparation de ce plan ».

Le paragraphe .09 - précise que « les aspects que le commissaire aux comptes prend en compte pour élaborer son plan de mission concernent notamment :

- la connaissance générale de l'entité…,
- la compréhension des systèmes comptable et de contrôle interne…,
- le risque d'audit et le seuil de signification… ».

La prise en compte de l'aspect informatique dans le plan de mission s'effectue sur la base des informations recueillies précédemment, lors des phases 1.1 « Prise de connaissance de l'informatique dans l'entreprise » et 1.2 « Description du système d'information », et qui portent sur :

- l'existence ou non d'une stratégie informatique,
- les caractéristiques de l'organisation informatique,
- l'importance de l'informatique dans l'entreprise,
- la complexité du système d'information,
- le nombre de processus et applications informatiques concernées.

Les informations obtenues et les risques potentiels identifiés doivent permettre de déterminer la nature et l'étendue des contrôles à mettre en œuvre.

Concernant la fonction informatique de l'entreprise, des faiblesses identifiées au niveau de l'organisation conduiront à une étude approfondie de l'incidence sur le risque inhérent. Lorsque les faiblesses concernent la formation des utilisateurs, cette étude sera essentiellement axée sur les aspects suivants : la distribution et le support informatique (cf. paragraphe 2.1.2 de la méthodologie) et la gestion de la sécurité (cf. paragraphe 2.1.3 de la méthodologie).

Lorsque l'informatique a une place importante dans l'entreprise, c'est-à-dire que l'environnement est très dématérialisé et qu'un arrêt brutal du système d'information aurait des conséquences déterminantes sur la poursuite des activités, le commissaire aux comptes veillera à apprécier d'une manière suffisamment complète les incidences possibles sur le risque inhérent et sur le risque lié au contrôle.

La complexité du système d'information est un élément important à considérer pour estimer la nécessité de faire intervenir un expert ou non. La norme CNCC 2-503 « Utilisation des travaux d'un expert » précise dans le paragraphe .07 - que « lorsque le commissaire aux comptes envisage de recourir à un expert, il prend en considération :

- l'importance relative dans les comptes de l'élément concerné,
- le risque d'erreur dû à la nature et à la complexité de l'élément concerné, et
- la quantité et la qualité des autres éléments probants disponibles ».

Comme le rappelle la norme, il est important de choisir un expert compétent et indépendant qui effectuera ses travaux sur la base des instructions communiquées par le commissaire aux comptes, la responsabilité de la mission incombant à ce dernier. Il est donc nécessaire que le commissaire aux comptes définisse précisément les travaux liés à la vérification du système informatique confiés à l'expert, ainsi que les résultats attendus.

Ces travaux concernent essentiellement les contrôles détaillés de la phase « Evaluation des risques », ainsi que les techniques d'audit assistées par ordinateur utilisées généralement dans la phase

« Obtention d'éléments probants ». Plus rarement, l'expert pourra également être sollicité au niveau de la phase « Orientation et planification de la mission », pour établir la cartographie d'applications.

Pour établir le cahier des charges des travaux confiés à l'expert, le commissaire aux comptes pourra utiliser utilement les informations présentées dans ce guide d'application, notamment pour préciser les résultats à atteindre. Le risque principal lié à l'intervention d'un expert informatique est d'obtenir des résultats qui soient inexploitables ou inadaptés pour l'expression de l'opinion.

Les supports opérationnels présentés en annexe, en particulier les exemples de feuilles de travail, ainsi que les fiches de mise en œuvre du chapitre « Techniques d'audit assistées par ordinateur » pourront être communiqués à l'expert pour fixer son intervention dans le cadre de la méthodologie et pouvoir intégrer directement ses travaux dans le dossier de travail.

Le nombre de processus identifiés et d'applications informatiques associées permet de définir les contrôles à mener dans la phase 2.2 « Incidence sur le risque lié au contrôle ». Il s'agit en effet d'étudier en priorité le ou les processus ayant un impact important sur l'émission de l'opinion, en raison du rôle joué dans l'établissement des comptes, du nombre d'applications concernées, ou des risques potentiels existants.

La phase « Evaluation des risques » est organisée en deux parties :
- incidence de l'environnement informatique sur le risque inhérent,
- incidence de l'environnement informatique sur le risque lié au contrôle.

Par ailleurs, le commissaire aux comptes consacre un chapitre de son plan de mission portant sur le respect de l'environnement légal et réglementaire lié à l'informatique, en application de la norme CNCC 2-206.

La norme CNCC 2-106 « Prise en compte des textes légaux et réglementaires » prévoit que :
- « le commissaire aux comptes planifie et conduit sa mission en faisant preuve d'esprit critique et en gardant à l'esprit que ses contrôles peuvent mettre en évidence des conditions ou des événements conduisant à s'interroger sur le non respect par l'entité des textes légaux et réglementaires » (paragraphe 12),
- « lors de la planification de sa mission, le commissaire aux comptes prend connaissance du cadre légal et réglementaire dans lequel s'inscrit l'entité et son secteur d'activité, et apprécie dans quelle mesure elle s'y conforme » (paragraphe 13),
- « après avoir acquis cette connaissance générale » (des textes légaux et réglementaires) « le commissaire aux comptes met en œuvre des procédures visant à identifier des cas possibles de non respect des textes légaux et réglementaires qu'il conviendrait de considérer lors de la préparation des comptes » (paragraphe 16).

Les cas possibles de non respect des textes légaux et réglementaires dans le domaine informatique, qu'il conviendrait de considérer lors de la préparation des comptes et que le commissaire aux comptes vise à identifier au travers de ses procédures proviennent, par exemple des :

- réglementations fiscales (Contrôle Fiscal Informatisé),
- déclarations CNIL,
- réglementations sur la propriété intellectuelle,
- réglementations sectorielles (banques, assurances, …).

L'identification de cas de non respect des textes légaux et réglementaires peut provenir :

- de la connaissance du commissaire aux comptes sur les pratiques de l'entreprise en termes d'informatique (dématérialisation des factures, chiffrement des courriers électroniques…) soumises à des réglementations spécifiques,
- de la prise de connaissance des documents suivants :
  - plan d'archivage des données informatisées,
  - déclarations CNIL,
  - liste des licences dont dispose l'entreprise,
  - documentation du système d'information,
- des entretiens avec les personnes suivantes :
  - direction de l'entreprise,
  - responsable informatique,
  - responsable sécurité,
  - responsable du service juridique.

Le commissaire aux comptes obtient par ailleurs une déclaration écrite de la direction confirmant qu'il a été informé de tous les cas survenus ou potentiels de non respect des textes légaux et réglementaires, dont les conséquences devraient être prises en considération lors de l'établissement des comptes.

Le respect des obligations externes en matière informatique peut s'apprécier à partir des réglementations suivantes :

- contrôle fiscal informatisé :
  - obligation de conservation des données et des traitements informatiques : les Brigades de Vérification des Comptabilités Informatisées (BVCI) de l'administration fiscale peuvent réaliser des investigations sur les données et les traitements informatiques de l'entreprise,
  - obligation de documentation des systèmes d'information : la documentation doit retracer les phases de conception, d'exploitation et de maintenance du système d'information. Elle doit expliquer l'architecture fonctionnelle et technique du système d'information, ainsi que les règles de gestion des données et des fichiers,
- informatique et libertés : l'entreprise doit effectuer la déclaration des fichiers nominatifs auprès de la CNIL (Commission Nationale des Informatiques et des Libertés),
- propriété intellectuelle : l'entreprise doit respecter les conditions d'utilisation des logiciels, notamment :
  - la loi relative aux droits d'auteur,
  - l'interdiction de reproduire ou d'utiliser des logiciels sans autorisation : l'entreprise doit disposer de contrats de licence d'utilisation pour chaque logiciel dont elle dispose,
- réglementations sectorielles appropriées : exemple, dans le secteur bancaire, respect de la réglementation du CRBF (Comité de la Réglementation Bancaire et Financière) relative au contrôle interne notamment l'organisation comptable et le traitement de l'information, le système de documentation et d'information (existence d'un manuel de procédures).

Les différents points abordés ci-dessus sont présentés de manière détaillée dans le Dossier thématique « Les obligations réglementaires ».

Les situations suivantes peuvent être rencontrées :

- archivage fiscal :
  - l'entreprise a défini l'ensemble des fichiers à archiver, la durée de conservation et procède régulièrement à des tests de reprise des données. Toutes les archives sont correctement documentées,
  - l'entreprise archive des données, mais le logiciel utilisé dans les exercices précédents n'est plus disponible : l'entreprise n'a pas la garantie de pouvoir récupérer les données. Risque que les données archivées ne soient pas récupérables,
  - aucune réflexion sur l'archivage des données n'a été menée dans l'entreprise. Risque que des données nécessaires n'aient pas été conservées,

- CNIL :
  - l'entreprise détient des données personnelles, mais ne les communique pas à l'extérieur et a procédé à une déclaration CNIL pour leur ensemble. Elle procède à des contrôles réguliers concernant les éventuelles modifications intervenant dans la collecte ou le traitement des données,
  - l'entreprise détient des données personnelles, ne les a pas déclarées à la CNIL, mais ne les utilise qu'en interne et les conserve dans des fichiers sécurisés. Risque de plaintes de la part des personnes répertoriées dans la liste et de sanctions pénales,
  - l'entreprise détient des données personnelles, ne les a pas déclarées à la CNIL et les communique à l'extérieur. Risque de plaintes de la part des personnes répertoriées dans la liste et de sanctions pénales,

- propriété intellectuelle :
  - l'entreprise détient les licences de toutes les applications qu'elle utilise,
  - l'entreprise utilise librement des images et textes soumis à des droits d'auteur dans des documents communiqués à l'extérieur. Risque de pénalités financières,
  - l'entreprise ne détient pas les licences de tous les logiciels installés sur les postes de travail. Risque de pénalités financières.

Les situations de non respect identifiées, le cas échéant, par le commissaire aux comptes le conduiront à apprécier leurs incidences potentielles sur les comptes. Le non respect d'une réglementation peut en effet impliquer des conséquences financières et parfois pénales pour l'entreprise et ses dirigeants.
Dans ce dernier cas, le commissaire aux comptes établira un lien éventuel avec son obligation de révélation de faits délictueux (cf. norme CNCC 6-701 « Révélation des faits délictueux au procureur de la République »).
Les cas de non respect relevés, constituant des irrégularités, conduisent également le commissaire aux comptes à faire un lien approprié avec ses obligations de communication avec les personnes constituant le gouvernement d'entreprise (cf. norme CNCC 2-107) et de communication à l'assemblée générale (cf. norme CNCC 5-112).

Exemple : une société n'ayant pas archivé les fichiers nécessaires pour pouvoir répondre aux requêtes demandées par les Brigades de Vérification des Comptabilités Informatisées, ou ne pouvant reconstituer les données des exercices précédents, peut être redressée pour rejet de comptabilité et se voir infliger des pénalités forfaitaires.

Une attention particulière doit être portée sur les données traitées sur un système informatique obsolète et plus utilisé dans l'entreprise. La reprise des données pourrait nécessiter la réinstallation du système, opération qui n'est pas toujours possible.

2. EVALUATION DES RISQUES

La phase « Evaluation des risques » a pour objectif la prise en compte de l'environnement informatique sur le risque inhérent et le risque lié au contrôle.

Elle intervient pour préparer et alléger les contrôles substantifs menés à la clôture des comptes et représente la phase la plus conséquente de l'ensemble de la mission.

Les travaux consistent à évaluer les risques en tenant compte de l'identification des risques potentiels et du système de contrôle interne mis en place par l'entreprise, et à en déduire la nature et l'étendue des contrôles substantifs à mener en phase « Obtention d'éléments probants » (à l'aide ou non de techniques d'audit assistées par ordinateur), afin de maintenir le risque d'audit à un niveau faible acceptable.

2.1. Incidence de l'environnement informatique sur le risque inhérent

L'incidence de l'environnement informatique sur le risque inhérent s'apprécie au regard des éléments suivants :

- la conception et l'acquisition des solutions informatiques,
- la distribution et le support informatique,
- la gestion de la sécurité,
- la gestion des projets informatiques.

Les caractéristiques de l'environnement informatique d'une entreprise peuvent entraîner un risque inhérent élevé et avoir une conséquence à terme sur la continuité d'exploitation. Une entreprise fortement dépendante de son informatique peut voir remise en cause son activité, en cas de défaillance majeure survenant dans son système d'information.

Même si l'incidence de l'environnement informatique n'est pas aussi souvent déterminante, la connaissance des processus informatiques permet :

- la mise en valeur de risques qui ne sont pas forcément décelables au niveau des applications, car transverses à l'ensemble du système d'information,
- une meilleure appréciation de l'incidence de l'informatique sur le risque lié au contrôle.

2.1.1. Conception et acquisition des solutions informatiques

A. Comment sont achetées ou développées les solutions informatiques ?

Objectif

Etudier les modalités d'achat ou de développement des solutions informatiques pour déterminer leur incidence sur le risque inhérent. L'entreprise doit avoir mis en place des procédures permettant d'identifier les besoins informatiques et de mener à terme les projets d'achats ou de développement de solutions.

Travaux à réaliser

L'étude consiste à vérifier que :
- les besoins en nouveaux outils sont correctement identifiés,
- une fonction développement distincte est prévue dans la structure informatique de l'entreprise,
- les développements / paramétrages suivent des procédures formalisées :
  - rédaction de cahier des charges / spécifications,
  - validations par la direction ou le responsable informatique,
- les procédures de tests sont définies :
  - environnement de tests spécifique,
  - tests formalisés avant la mise en production.

Modalités pratiques

L'étude peut s'appuyer :
- sur les documents suivants :
  - procédures de développement (langage utilisé, syntaxe, environnement utilisé…),
  - dossier de paramétrage,
  - contrats de sous-traitance de solutions informatiques,
- sur les entretiens avec le responsable informatique, le responsable du développement ou du paramétrage.

L'incidence des modalités d'achat ou de développement des solutions informatiques sur le risque inhérent peut s'apprécier à partir des éléments suivants :
- existence de procédures visant à identifier les besoins en nouveaux outils et/ou solutions informatiques et à définir des choix :
  - suivi des performances du système d'information en place,
  - procédures et modalités de choix des nouveaux outils,
  - processus de prise de décision (fixation du budget, validation des projets d'investissement) et implication de la direction dans ce processus,
- rédaction des spécifications pour le développement / paramétrage de nouveaux outils :
  - rédaction du cahier des charges en collaboration avec les utilisateurs du futur outil,
  - spécifications écrites détaillées pour chaque développement ou modification,
  - participation des responsables opérationnels dans la validation des spécifications,
- suivi des projets en cours, de mise à jour, acquisition, développement et maintenance des applications :
  - suivi des coûts engagés par rapport aux coûts budgétés,
  - suivi du respect des délais (rétro-planning, jalons intermédiaires…),
  - suivi des interventions des prestataires externes.

L'incidence des modalités d'achat ou de développement des solutions informatiques sur le risque inhérent peut être schématisée comme suit, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Identification des besoins en nouveaux outils	La performance des outils est suivie régulièrement par le responsable informatique (indisponibilités, pannes, temps de réponse…). Des enquêtes auprès des utilisateurs permettent de recueillir leurs besoins.	Le responsable informatique effectue une veille technologique et procède aux changements de matériel suivant un plan préétabli, mais il ne suit pas les performances des outils existants. *Risque de pannes avec nécessité d'un changement de matériel en urgence en plus du plan de remplacement prévu.*	Le matériel n'est changé que lorsque surviennent des pannes majeures. *Risque de pannes bloquantes non anticipées avec un temps de latence avant réparation.*
Organisation de la fonction développement / paramétrage	Une équipe dédiée au développement / paramétrage a été désignée.	Le responsable informatique est également responsable du développement / paramétrage. *Risque de fraudes et de manque de supervision des travaux effectués.*	Aucun responsable du développement / paramétrage n'a été désigné. *Risque de besoins en développement / paramétrage non pris en compte et risque d'incohérence dans les projets.*
Procédures de développement / paramétrage	Des procédures écrites détaillent qui a accès aux environnements de développement / paramétrage, les normes à respecter, les procédures de tests et de mise en production.	Les procédures de développement / paramétrage sont connues par l'équipe responsable, mais elles n'ont pas fait l'objet d'une formalisation. *Risque que les développements/ paramétrages soient insuffisamment documentés et mal coordonnés.*	Aucune procédure de développement / paramétrage n'a été mise au point. *Risque de méthodes de développement / paramétrage incohérentes selon les intervenants.*
Procédures de tests	Des procédures sont appliquées pour effectuer les tests dans un environnement spécifique, pour conserver le mode opératoire utilisé et les résultats (fiches de recette visées par le responsable).	Des tests sont menés sans être formalisés : aucun archivage des résultats de tests après leur mise en œuvre. *Des zones de risques peuvent être oubliées lors de la phase de tests, d'où un risque d'anomalies non détectées.*	Le déploiement est effectué sans procédure de tests. *Risque d'anomalies non détectées.*

Résultat

L'étude des éléments précédents permet de déterminer l'incidence des processus de conception et d'acquisition des solutions informatiques sur le risque inhérent, se traduisant par exemple par :

- des irrégularités dans l'attribution de marchés informatiques,

- des incohérences du système d'information liées au choix et au développement d'applications non pertinentes par rapport au système d'information existant, impliquant une perte de maîtrise ou une incapacité du système d'information à évoluer correctement,
- des surcoûts financiers liés au choix d'une solution pour laquelle il n'existe pas en interne d'informaticien capable de la maintenir et impliquant une augmentation des charges pour l'entreprise et une baisse de la trésorerie.

Exemple :

On observe très fréquemment que les filiales de groupes se voient imposer une application, sans qu'elles interviennent dans ce choix. Les solutions mises en place sont souvent très lourdes pour des petites et moyennes entreprises et les fonctionnalités des logiciels imposés pas toujours adaptées aux besoins des utilisateurs.
La conséquence immédiate est le coût important que représente le projet pour la filiale, surtout si le groupe n'apporte pas son soutien financier.
En outre, les contraintes liées à un progiciel d'une certaine taille ne sont pas souvent adaptées aux spécificités fonctionnelles, à la réactivité d'une petite et moyenne entreprise. La mise en place d'un tel système peut, dans certains cas, entraîner de graves dysfonctionnements dans l'organisation de l'entreprise et avoir des conséquences sur sa rentabilité. Le commissaire aux comptes peut sensibiliser les dirigeants d'entreprises à de telles conséquences.

B. Comment sont installés et validés les nouveaux systèmes informatiques ?

Objectif

Etudier les modalités d'installation et de validation des nouveaux systèmes informatiques pour déterminer leur incidence sur le risque inhérent. L'entreprise doit avoir mis en place des procédures de gestion de projet pour permettre une mise en place sans risque d'un nouvel outil ou d'une nouvelle application.

Travaux à réaliser

L'étude consiste à vérifier que :

- l'entreprise effectue des tests avant le démarrage de toute nouvelle application ou d'une nouvelle version,
- les développements sont validés par la direction ou le responsable informatique avant d'être déployés,
- le niveau de documentation des outils est approprié,
- des méthodes de gestion du changement sont prévues pour faciliter le démarrage.

Modalités pratiques

L'étude peut s'appuyer :

- sur l'analyse des documents suivants :
  - inventaire des solutions informatiques,
  - calendrier des tests de validation,
  - fiches de recette/comptes-rendus des tests,
- sur les entretiens avec les personnes suivantes :
  - responsable informatique,
  - responsable du développement,
  - utilisateurs ayant participé à la recette,
  - responsables opérationnels associés au projet.

L'incidence des modalités d'installation et de validation des nouveaux systèmes informatiques sur le risque inhérent peut s'apprécier à partir des éléments suivants :

- existence de procédures de tests avant mise en production :
  - une nouvelle application (logiciel ou progiciel) doit être contrôlée en environnement de test par des utilisateurs afin de valider son adéquation aux besoins,
  - lors du remplacement d'un logiciel par un nouveau logiciel, il est préférable de conserver les deux logiciels et de gérer en parallèle l'ancien et le nouveau afin de s'assurer du correct fonctionnement de la nouvelle application,
- séparation des environnements de développement, de test et d'exploitation :
  - un logiciel en cours de développement ou en test ne doit pas pouvoir être utilisé pour la gestion des données réelles et ne doit pas être accessible aux utilisateurs,
  - les développeurs n'ont pas à avoir accès aux logiciels en environnement de production,
- suivi et documentation des modifications mises en œuvre, afin de garder une trace de toutes les évolutions du système d'information, avec les dates et les personnes ayant réalisé la modification,
- tests liés au démarrage de la nouvelle application ou de la nouvelle version d'une application :
  - tests de performance du nouvel outil,
  - tests des fonctionnalités sur un échantillon réduit d'utilisateurs,

  - tests de traitements en parallèle des données sur l'ancien et le nouveau système,
  - tests sur les traitements internes à l'outil, la sécurité, les interfaces avec d'autres outils, les résultats produits par le nouvel outil,
- validation des développements effectués avant déploiement :
  - par la direction de l'entreprise,
  - par le responsable informatique,
- gestion du changement :
  - information du personnel de l'entreprise (courriers électroniques, notes internes…),
  - organisation d'un plan de formation à l'attention des utilisateurs,
  - manuel d'utilisation rédigé (mode opératoire),
  - mise en place d'une cellule de support aux utilisateurs,
  - questionnaires de satisfaction auprès des utilisateurs.

L'incidence des modalités d'installation et de validation des nouveaux systèmes informatiques sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Tests lors du démarrage de la nouvelle application ou version	De nombreux tests sont effectués lors de l'installation et après l'installation en menant des enquêtes auprès des utilisateurs, ou en déployant l'outil pour un échantillon d'utilisateurs testeurs.	Des tests sont effectués mais ne sont pas formalisés : aucune trace de ces tests n'est conservée. *Des zones de risques peuvent être oubliées lors de la phase de tests, d'où un risque d'anomalies non détectées.*	Aucun test n'est effectué dans cette phase du projet : seuls les tests lors de la phase de développement sont utilisés. *Risque d'anomalies non détectées.*
Validation des développements	Le responsable informatique rédige et signe une fiche de recette validant le développement.	La personne visant les fiches de recette qui donne le feu vert fait partie de l'équipe opérationnelle de développement. *Risque que des erreurs ne soient pas décelées par manque de supervision extérieure.*	Les tests ne sont pas centralisés et aucune fiche de recette ne vient donner le « feu vert » au déploiement. *Des zones de risques peuvent être oubliées lors de la phase de tests, d'où un risque d'anomalies non détectées.*
Niveau de documentation des outils	Une documentation complète décrivant l'outil, le cahier des charges et les spécifications, les tests mis en œuvre, est à jour et disponible.	Seule est disponible une description succincte de l'outil. *Risque de mauvaise connaissance de l'outil et de ses fonctionnalités complètes.*	Aucune documentation écrite n'est disponible sur l'outil développé. *Risque de perte de connaissances sur les phases de conception de l'outil et sur les anomalies constatées.*
Gestion du changement	Un programme de formation à l'ensemble des utilisateurs est mis en place. Des notes internes de sensibilisation aux impacts du nouvel outil sont envoyées à l'ensemble du personnel. Une cellule de support aux utilisateurs a été	Les utilisateurs sont prévenus par notes internes des changements occasionnés par le nouvel outil sans organiser un programme de formation. *Risque que des utilisateurs ne se sentent pas concernés ou qu'ils ne disposent pas de la*	Aucune information, ni formation provenant de la direction n'est dispensée aux utilisateurs. *Risque de mauvaise utilisation des nouveaux outils.*

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
	créée pour répondre à leurs interrogations.	*totalité des informations nécessaires.*	

Résultat

L'étude des éléments précédents permet de déterminer l'incidence sur le risque inhérent des processus d'installation et de validation des nouveaux systèmes informatiques (liée aux méthodes de mises en production retenues et à la taille du projet). De la taille du projet et de sa « couverture métier » (implication d'un ou plusieurs services de l'entreprise), dépendra le niveau de risque pour l'entreprise.
La mise en production d'une application mal ou insuffisamment testée peut avoir des conséquences directes sur l'établissement des comptes. Si le système d'information présente des failles de conception, les comptes pourront contenir des anomalies.

Exemple

Une société de production et de négoce de champagne a mis en place une nouvelle application de gestion des ventes. Faute de temps, l'application a été testée rapidement et seuls les principaux types de vente ont été testés.
L'application a été mise en production quelques mois avant la fin de l'année qui est la période au cours de laquelle 70 % du chiffre d'affaires est réalisé.
Au mois de décembre, alors que l'activité était maximale, les commerciaux se sont aperçus qu'il était impossible d'enregistrer dans l'application les ventes de bouteilles en coffret (une bouteille de Champagne plus une bouteille de vin). En effet, cette fonctionnalité n'avait pas été testée et ne fonctionnait pas dans la nouvelle application. Toutes les ventes de ce type ont donc été enregistrées manuellement sur un cahier et saisies par la suite en comptabilité. Le risque est la non exhaustivité des enregistrements et le non respect de la séparation des exercices qui aurait été évité si l'application avait fait l'objet de tests plus complets.
Cet exemple montre qu'une des difficultés est de recenser préalablement tous les cas de figures qui peuvent se présenter et pour lesquels une réponse doit être prévue et testée. Ainsi, la coopération des utilisateurs en amont du processus s'avère indispensable.

C. Comment est assurée la maintenance du système d'information ?

Objectif

Etudier les modalités de maintenance du système d'information pour déterminer leur incidence sur le risque inhérent. L'entreprise doit avoir mis en place des procédures permettant la continuité d'exploitation des applications, leur pérennité et leur disponibilité.
Les procédures doivent concerner le suivi des performances des applications et systèmes, un programme de révisions régulières, une procédure en cas de défaillance du système ou d'une application.

Travaux à réaliser

L'étude consiste à vérifier que :
- le département informatique a une bonne maîtrise de ses applications et est capable de les faire évoluer dans le temps, c'est-à-dire de les maintenir,
- le recours à une maintenance externalisée n'entraîne pas une dépendance trop forte de l'entreprise vis-à-vis de ses prestataires.

Modalités pratiques

L'étude peut s'appuyer :
- sur l'analyse des documents suivants :
  - journal des interventions du service maintenance / sous-traitance,
  - contrats de maintenance,
  - comptes-rendus d'intervention des sous-traitants,
- sur les entretiens avec les personnes suivantes :
  - responsable informatique,
  - responsable de la fonction maintenance/exploitation,
  - responsables fonctionnels (ventes, achats, comptabilité, …).

L'incidence des modalités de maintenance du système d'information sur le risque inhérent peut s'apprécier à partir des éléments suivants :
- suivi des performances du système d'information afin de détecter les points de faiblesse du système :
  - suivi des pannes et des indisponibilités (fréquence, temps d'indisponibilité),
  - analyse des états d'anomalies,
  - suivi des incidents déclarés par les utilisateurs,
- connaissance de l'existant : la maîtrise du parc informatique est un élément essentiel. Pour cela, il peut être vérifié que le responsable informatique :
  - connaît l'environnement général informatique,
  - connaît les applications utilisées dans l'entreprise,
  - utilise des outils de gestion de parc informatique,
- en cas de maintenance externalisée, des procédures de suivi de l'activité des prestataires externes doivent être mises en place :
  - comparaison des résultats avec la prestation attendue (obligations contractuelles en termes de temps d'intervention et de remise en marche),
  - comptes-rendus systématiques d'interventions.

L'incidence des modalités de maintenance du système d'information sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Maîtrise du système d'information	Le responsable informatique utilise des outils de suivi permettant de surveiller les performances du système, de connaître le parc informatique, de vérifier les applications installées sur les postes de travail.	Le responsable informatique fait des tests ponctuels sur les machines et connaît les principaux incidents survenus, mais ne dispose d'aucun outil de suivi automatisé. *Risque que les tests ne soient pas exhaustifs, que surviennent des pannes non anticipées et/ou non traitées.*	Le responsable n'a pas une connaissance suffisante du parc informatique, ni de la cartographie complète des applications utilisées dans l'entreprise. Il ne suit pas les indisponibilités du système. *Risque de perte de contrôle du système d'information et d'incidents non anticipés.*
Maintenance externalisée	Le prestataire surveille régulièrement les indisponibilités du système. En cas de panne il intervient rapidement : son niveau de service est conforme au niveau de service attendu précisé dans son contrat. Il remet à l'entreprise des comptes-rendus de ses interventions.	Le prestataire accomplit les prestations prévues dans le contrat, mais le délai d'intervention est trop important. *Risque de perturbations dans le fonctionnement courant de l'entreprise.*	Le prestataire n'est pas adapté à la taille de l'entreprise. Il ne se déplace pas pour toutes les interventions demandées et ses temps de réponse sont trop importants. Aucun niveau de service n'est prévu dans le contrat et les conditions de rupture de contrats ne sont pas détaillées. *Risque d'indisponibilité longue des systèmes et d'une qualité de service non satisfaisante, sans que la responsabilité du prestataire puisse être engagée.*

Résultat

L'étude des éléments précédents permet de déterminer l'incidence des modalités de maintenance du système d'information sur le risque inhérent, se traduisant par exemple par :

- la perte de maîtrise des outils informatiques par l'entreprise. Le risque de perte de maîtrise est important si l'application est mal documentée et si les personnes l'ayant conçue viennent à quitter l'entreprise (retraite, licenciement, prestataire en cessation d'activité),
- une forte dépendance de l'entreprise vis-à-vis de tiers pour faire évoluer ses systèmes d'information : il en découle un risque de dysfonctionnement grave ou de perturbation pouvant avoir une incidence sur la poursuite d'activité.

Exemple

Une société intervenant sur un secteur d'activité très ciblé a fait développer par un prestataire une application de gestion d'actifs financiers. Cette application est très spécifique et le prestataire l'adapte en permanence aux besoins exprimés par les utilisateurs qui doivent être très réactifs face au marché.
La documentation des développements réalisés par le prestataire informatique est inexistante. La société est donc totalement dépendante de son prestataire, car en cas de défaillance personne ne sera en mesure de faire évoluer l'application. La société ne pourra alors plus suivre de façon aussi réactive les évolutions du marché et rencontrera des difficultés à comptabiliser les opérations complexes.

2.1.2. Distribution et support informatique

A. Quelle est la qualité du support fourni aux utilisateurs ?

Objectif

Etudier la qualité du support fourni aux utilisateurs pour déterminer son incidence sur le risque inhérent. L'entreprise doit avoir mis en place un dispositif de formation et d'assistance permettant aux utilisateurs d'avoir les connaissances nécessaires pour une utilisation optimale des outils dont ils ont l'usage dans le cadre de leurs fonctions. Ainsi, pour chaque nouvel outil, un support aux utilisateurs et/ou une formation doivent être dispensés, afin de réduire le risque de mauvaises utilisations (erreurs, traitements inadaptés…).

Travaux à réaliser

L'étude consiste à vérifier que :

- les utilisateurs disposent d'une information suffisante sur les outils qu'ils utilisent :
  - formation aux nouveaux outils / formation à l'informatique,
  - documentation et manuel utilisateur disponibles à tout moment,
  - possibilité de faire appel à une cellule de support,
- les procédures de formation sont adaptées (formation initiale / formation continue).

Modalités pratiques

L'étude peut s'appuyer :

- sur l'analyse des documents suivants :
  - plans de formation collectifs / individuels,
  - demandes de formation (acceptées/refusées),
  - évaluation des formations reçues par les participants,
  - journal des demandes des utilisateurs au support informatique,
  - journal de suivi des incidents / résolutions par le support informatique,
- sur les entretiens avec les personnes suivantes :
  - direction de l'entreprise,
  - responsable informatique,
  - responsable de la formation / Responsable des ressources humaines,
  - responsable du support informatique aux utilisateurs.

L'incidence de la qualité du support fourni aux utilisateurs sur le risque inhérent peut s'apprécier à partir des éléments suivants :

- mise en place d'une cellule de support aux utilisateurs :
  - suivi des appels / traitement des anomalies,
  - statistiques sur les types de questions posées,
- mise en place d'un plan de formation :
  - remontée des demandes de formation,
  - plans de formation individuels et collectifs.

L'incidence de la qualité du support fourni aux utilisateurs sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Cellule de support (hot line ou help desk)	Une cellule dédiée au support utilisateurs existe et est opérationnelle pendant l'ensemble du temps de travail.	Cellule de support peu disponible au cours de la journée. *Risque de non prise en compte systématique des problèmes rencontrés par les utilisateurs, pouvant être à l'origine d'erreurs d'utilisation non corrigées.*	Aucune cellule de support créée. *Risque que des cas rencontrés par les utilisateurs ne soient pas résolus, pouvant être à l'origine d'erreurs d'utilisation. Risque que des anomalies rencontrées par les utilisateurs ne puissent pas être traitées.*
Manuel utilisateur et documentations disponibles	Une documentation complète et l'ensemble des manuels utilisateurs des outils informatiques sont disponibles et mis à jour en permanence.	Une documentation est disponible mais elle n'est pas à jour. *Risque que de nouvelles fonctionnalités ne soient pas connues des utilisateurs, pouvant être à l'origine d'erreurs d'utilisation.*	Le personnel ne dispose d'aucune documentation sur les outils informatiques dont il a l'utilisation. *Risque de connaissance insuffisante des fonctionnalités de l'outil par les utilisateurs, pouvant être à l'origine d'erreurs d'utilisation.*
Formations informatiques	Des procédures permettent aux utilisateurs de demander des formations adaptées à leur niveau de compétence. Un cursus de formation informatique leur est imposé lors du lancement de nouveaux outils.	Des formations informatiques peuvent être prises en charge par l'entreprise sur demande des utilisateurs. *Risque que les demandes des utilisateurs ne remontent pas systématiquement aux responsables concernés.*	Aucune formation informatique n'est dispensée aux utilisateurs. *Risque que les outils informatiques ne soient pas correctement utilisés par manque de formation.*

Résultat

L'étude des éléments précédents permet de déterminer l'incidence du support utilisateurs sur le risque inhérent, résultant de faiblesses dans la qualité de la formation et dans la maîtrise par les utilisateurs de l'outil, souvent responsables de nombreux dysfonctionnements attribués à un logiciel.
Il pourra alors être recommandé l'amélioration du contrôle interne par des actions de formation et la mise en place de nouveaux états de contrôle.

Exemple

Suite à la mise en place d'un progiciel, l'organisation du contrôle interne est perturbée. Les utilisateurs ne connaissent pas les états à utiliser pour réaliser les contrôles qu'ils pratiquaient précédemment.
La conséquence peut être qu'ils ne réalisent plus aucun contrôle, effectuent des opérations erronées (de nombreuses anomalies étant constatées au niveau des interfaces entre applications), ou encore réalisent des contrôles non pertinents ou superflus.
Une attention particulière doit être portée à la mise en place d'un progiciel de gestion intégré dans une entreprise. En effet, cette installation, outre les problématiques habituelles de prise en main d'un

nouvel outil informatique, suscite également un changement profond dans l'organisation du travail, les contrôles et les responsabilités de chaque intervenant.

B. Comment sont gérés les problèmes d'exploitation quotidiens ?

Objectif

Etudier les modalités d'exploitation du système d'information pour déterminer leur incidence sur le risque inhérent. L'administrateur du système d'information est responsable du bon fonctionnement de ce système et de son contrôle. C'est à lui de centraliser les anomalies ou dysfonctionnements des éléments composant l'architecture. Il gère les habilitations d'accès aux données et doit pouvoir détecter les tentatives d'intrusion. Son rôle est primordial dans la prévention des risques informatiques.
L'ensemble de ces tâches doit être régulièrement effectué par un administrateur désigné afin de permettre la pérennité du système d'information, sa fiabilité et la disponibilité de l'information.

Travaux réalisés

L'étude consiste à :
- analyser les procédures de suivi des dysfonctionnements du système d'information :
  - suivi des pannes/indisponibilités,
  - suivi de la volumétrie,
  - suivi des indicateurs de performance,
- vérifier qu'une fonction exploitation spécifique existe et assure une disponibilité satisfaisante du système d'information,
- vérifier que des états d'alerte sur l'exploitation existent, sont édités et analysés.

Modalités pratiques

L'étude peut s'appuyer sur les documents suivants :
- procédures formalisées d'exploitation,
- états d'anomalies des systèmes,
- suivi des performances du système d'information,
- statistiques de connexions et d'anomalies,
- liste des profils existants / liste des habilitations par utilisateurs.

L'incidence des modalités d'exploitation du système d'information sur le risque inhérent peut s'apprécier par l'étude des habilitations et des états d'anomalies.

Gestion des habilitations :
- suivi des comptes utilisateurs : recherche de comptes non utilisés qui peuvent être des points d'entrée potentiels pour des fraudeurs,
- existence de comptes communs : les comptes communs doivent être évités car ils ne permettent pas de savoir quel utilisateur a agi sous ce compte lors de l'analyse des états de connexion,
- fiabilité des identifiants et mots de passe : des outils permettent de rechercher les mots de passe trop faciles à découvrir (mots du dictionnaire, prénoms, mots de passe égaux à l'identifiant),

- gestion de niveaux d'habilitation différents selon les postes occupés, comme par exemple :
  - habilitations en écriture sur l'application de comptabilité pour l'équipe comptable et en consultation seule pour le reste des salariés,
  - habilitations en consultation des données salariales aux seules équipes de paye et à la direction.

Revue régulière des états d'anomalies d'exploitation, analyse et suivi des incidents :

- tous les incidents doivent pouvoir être détectés et corrigés avant qu'ils n'entraînent des destructions ou altérations de données,
- les états de connexion doivent également être suivis :
  - les connexions en dehors des heures de travail normales doivent pouvoir être expliquées,
  - des tentatives répétées d'accès sous des mots de passe différents doivent pouvoir être détectées et bloquées.

L'incidence des modalités d'exploitation du système d'information sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Suivi des performances du système	L'administrateur du réseau surveille chaque jour les pannes, indisponibilités, et temps de réponse des outils. Il renseigne régulièrement un récapitulatif des anomalies et de leur résolution.	Un responsable désigné doit suivre régulièrement ces indicateurs mais ses observations ne sont pas formalisées. *Risque que des anomalies décelées par le responsable ne soient pas suivies car non répertoriées.*	Aucun suivi des performances du système n'est effectué au sein de la structure. *Risque que des anomalies non anticipées surviennent nécessitant des solutions d'urgence.*
Disponibilité du système	Un outil informatique permet de recenser l'ensemble des temps d'indisponibilité du système. Les causes de l'indisponibilité doivent être expliquées. Cet indicateur doit rester faible et occasionnel.	Les indisponibilités du système sont occasionnelles mais ne sont pas expliquées. *Risque d'anomalie grave non décelée pouvant entraîner des pannes et des pertes de données.*	Les indisponibilités du système sont de plus en plus fréquentes mais ne sont pas surveillées. *Risque de panne bloquante et de perte de données.*
Fonction exploitation	Un administrateur et/ou une équipe chargée de l'exploitation à plein temps sont désignés. Ils effectuent les opérations de gestion et de surveillance du réseau quotidiennement.	Un administrateur est désigné mais occupe d'autres fonctions* dans l'entreprise et n'est pas toujours disponible pour occuper la fonction d'exploitation. *Risque que la fonction exploitation soit mal assurée, risque de perte du pilotage du système.* * A relativiser en fonction de la taille de l'entreprise.	Aucune personne n'est désignée pour occuper la fonction d'administrateur : le réseau n'est pas surveillé régulièrement. Toutes les machines ont des droits administrateurs et en conséquence, des applications peuvent être installées sans intervention d'un responsable. *Risque que le système ne fasse plus l'objet de contrôle.*
Historique et surveillance des activités	L'administrateur dispose des statistiques de connexions et	L'administrateur ne dispose pas de statistiques de connexions.	Un administrateur ne surveillant pas les connexions effectuées

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
	d'anomalies : il les analyse régulièrement et explique les incidents détectés.	*Risque que des connexions anormales ne soient pas décelées.*	pourrait ne pas détecter une éventuelle tentative d'intrusion. *Risque de tentative d'intrusion non détectée.*

Résultat

L'étude des éléments précédents permet de déterminer l'incidence des modalités d'exploitation du système d'information sur le risque inhérent, résultant d'un manque de maîtrise par l'entreprise de l'exploitation informatique quotidienne. Une équipe informatique doit être capable de résoudre rapidement les problèmes quotidiens, par exemple de coupures de ligne, d'arrêts du réseau informatique, de transferts de fichiers (le jour et la nuit).

Exemple

L'analyse des statistiques des outils informatiques de l'entreprise doit permettre de détecter des anomalies de façon préventive, telles que dans les cas suivants :

- des connexions au réseau de l'entreprise apparaissant dans les statistiques de connexions en fin de semaine ou la nuit peuvent permettre de déceler des accès non autorisés aux données de l'entreprise,
- des anomalies répétées au niveau d'une interface peuvent permettre de détecter une erreur de paramétrage,
- des temps de réponses anormalement élevés peuvent permettre de déceler une inadaptation des outils informatiques aux volumes de données à traiter,
- des incidents répétés peuvent représenter une alerte avant une panne sérieuse des outils informatiques utilisés dans l'entreprise.

C. Comment sont gérées les fonctions externalisées ?

Objectif

Etudier les modalités de gestion des fonctions externalisées pour déterminer leur incidence sur le risque inhérent. L'externalisation d'une fonction informatique est une solution qui est de plus en plus fréquemment utilisée par les entreprises.
Pour chaque fonction externalisée, un contrat écrit doit préciser les rôles et responsabilités de chaque partie, les prestations et le niveau de service attendus.
La fiabilité du prestataire choisi, l'adéquation de ses compétences avec les besoins de l'entreprise, la qualité des services rendus ainsi que sa pérennité constituent des éléments de référence importants : un contrat de prestation de services peu formalisé, ou un prestataire peu fiable, peut entraîner un risque de pertes financières et dans les cas les plus graves, un risque de continuité d'exploitation.

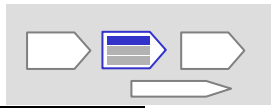
Travaux à réaliser

L'étude consiste à :
- obtenir la liste des contrats d'externalisation souscrits par l'entreprise,
- vérifier que les sous-traitants choisis correspondent aux besoins de l'entreprise :
  - analyser les procédures de choix et de validation du choix du sous-traitant,
  - analyser les caractéristiques des sous-traitants choisis,
- analyser les modes de supervision des travaux externalisés,
- analyser le contenu des contrats d'externalisation :
  - responsabilité des deux parties,
  - clauses de résiliation,
  - niveau de services attendu,
  - modalités de fin des prestations,
  - modalités d'échanges avec le prestataire, notamment en matière de délai, d'états souhaités, de documentation des systèmes.

Modalités pratiques

L'étude peut s'appuyer :
- sur l'analyse des documents suivants :
  - procédures de sélection d'un sous-traitant,
  - description des entreprises sous-traitantes,
  - liste des contrats d'externalisation de la société et contenu de ces contrats,
  - journal des interventions de sous-traitant et comptes-rendus de ces interventions,
- sur les entretiens avec les personnes suivantes :
  - direction de l'entreprise,
  - responsable informatique,
  - responsables d'entreprises sous-traitantes.

L'incidence des modalités de gestion des fonctions externalisées sur le risque inhérent peut s'apprécier à partir des éléments suivants :
- procédures relatives à la sous-traitance :
  - procédure de sélection d'un prestataire,
  - détection puis validation des besoins en sous-traitance avec la direction.
- liste des contrats de sous-traitance de la société et contenu de ces contrats :
  - niveaux de services qualitatifs et quantitatifs attendus,
  - clauses de résiliation du contrat,



  - délais d'intervention,
  - responsabilité des deux parties,
  - comptes-rendus du sous-traitant sur ses interventions,
- mode d'intervention du sous-traitant :
  - si le sous-traitant intervient en se connectant au réseau à distance, la sécurité des données est-elle assurée ?
  - si le sous-traitant intervient directement dans le système, à quelles données a-t-il accès ?
  - le contrat comporte-t-il une clause de confidentialité ?

L'incidence des modalités de gestion des fonctions externalisées sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Procédures de choix des sous-traitants	L'entreprise procède à des appels d'offres : la direction et le responsable informatique choisissent le sous-traitant en fonction de sa taille, de ses spécialités, ses références…	L'entreprise travaille avec les mêmes sous-traitants depuis longtemps et ne procède pas à des appels d'offres. *Risque que le choix du sous-traitant ne soit plus adapté aux besoins de l'entreprise ou que le sous-traitant détienne toute la connaissance de l'entreprise.*	L'entreprise n'a pas de procédure de choix des sous-traitants. *Risque que le choix du prestataire ne soit pas optimal (tarifs, domaine de compétences, taille ...)*
Sous-traitants correspondant aux besoins de l'entreprise	Les sous-traitants répondent aux besoins de l'entreprise, ont de l'expérience dans le type de prestation demandé, le niveau des prestations est conforme à l'objectif.	Le sous-traitant n'est jamais intervenu dans un environnement applicatif ou matériel similaire à celui de l'entreprise. *Risque que le sous-traitant ne parvienne pas à traiter toutes les tâches qui lui sont assignées ou que la qualité des prestations soit insuffisante.*	Le sous-traitant n'est pas disponible pour l'entreprise et ne parvient pas toujours à résoudre les problèmes qui lui sont posés. *Risque que des anomalies ne soient pas résolues et entraînent des dysfonctionnements importants.*
Supervision des activités des sous-traitants	Les sous-traitants doivent systématiquement remettre des comptes-rendus d'intervention et d'avancement. A chaque intervention, la conformité du résultat attendu par rapport aux travaux effectués est vérifiée.	Les sous-traitants ne sont pas tenus de remettre des comptes-rendus d'intervention systématiquement, mais ils sont en contact régulier avec le responsable informatique. *Risque que le sous-traitant intervienne sans réellement résoudre les anomalies rencontrées.*	Les interventions des sous-traitants ne sont pas surveillées et le résultat de leur prestation n'est pas comparé au résultat attendu. *Risque que le résultat des interventions du sous-traitant ne soit pas conforme au résultat attendu.*
Contenu des contrats de sous-traitance	Le contrat comporte des clauses de confidentialité, de fin de contrat, de niveau de services attendu, de suivi d'activité (indicateurs) et décrit précisément les	Le contrat décrit le type de prestation attendue, mais pas le niveau de service demandé. *Risque que la responsabilité du sous-traitant ne puisse pas être*	Le contrat ne présente pas les obligations des deux parties, ni les modalités de fin des prestations. Le contrat est signé par une personne non habilitée à engager l'entreprise.

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
	responsabilités des deux parties.	*invoquée si le niveau de service de la prestation est jugé insuffisant.*	*Risque que le contrat soit considéré comme nul en cas de mise en cause de la responsabilité d'une des deux parties dans l'hypothèse d'une mésentente.*

Résultat

L'étude des éléments précédents permet de déterminer l'incidence de l'externalisation d'une fonction informatique sur le risque inhérent, résultant :

- de l'inexistence ou de la faiblesse des contrats d'externalisation, pouvant entraîner une perte de contrôle ou une perte de maîtrise du système d'information si les modalités d'externalisation ne sont pas précisément définies,
- du niveau de dépendance et de supervision de l'entreprise par rapport au prestataire.

Exemple :

Une entreprise de petite taille sous-traite l'ensemble de sa fonction informatique à son ancien directeur informatique qui a créé sa société de conseil. Il intervient deux jours par semaine dans les locaux de l'entreprise et sur demande en cas de panne ou d'anomalies à traiter.
Le prestataire étant le seul à avoir la connaissance de l'environnement informatique de l'entreprise est rapidement devenu indispensable. Les tarifs des prestations augmentent et, étant seul dans son entreprise, le prestataire ne peut pas toujours être disponible immédiatement. De même, lorsque celui-ci est en congé, aucune personne ne peut intervenir à sa place en cas de panne ou d'incident. L'entreprise pourrait donc se trouver plusieurs semaines sans système d'information utilisable par suite d'indisponibilité du prestataire.

2.1.3. Gestion de la sécurité

A. Comment sont gérées les sauvegardes, existe-t-il un plan de secours ?

Objectif

Etudier la gestion de la sécurité pour déterminer son incidence sur le risque inhérent. L'entreprise doit avoir mis en place des procédures efficaces de sauvegarde et un plan de secours :

- procédures de sauvegarde : les données de l'entreprise doivent être correctement sauvegardées pour qu'en cas de défaillance du système d'information, ces données soient facilement récupérables,
- plan de secours : dans certains secteurs d'activité, l'entreprise doit prévoir une solution capable de se substituer au système d'information courant pour pouvoir faire face à un sinistre majeur.

Travaux à réaliser

L'étude consiste à :

- vérifier que des procédures de sauvegarde ont été établies et sont appliquées :
  - exhaustivité des applications sauvegardées,
  - fréquence des sauvegardes,
  - durée et lieu de conservation des données,
  - tests réguliers de relecture des supports de sauvegarde,
- vérifier que l'entreprise a mis en œuvre une réflexion sur les solutions de secours en cas de défaillance du système ou en cas de sinistre :
  - processus critiques,
  - plan de reprise d'activité,
  - site de repli.

Modalités pratiques

L'étude peut s'appuyer :

- sur l'analyse des documents suivants :
  - procédures de sauvegarde formalisées,
  - comptes-rendus des tests de reprise de données,
  - contrats de prestation de plan de secours,
  - charte de bonne utilisation du système d'information à destination des utilisateurs,
- sur les entretiens avec les personnes suivantes :
  - responsable de l'informatique,
  - responsable de la sécurité,
  - prestataire externe en charge des solutions de secours.

L'incidence des modalités de la gestion des sauvegardes sur le risque inhérent peut s'apprécier à partir des éléments suivants :

- procédures de sauvegardes régulières :
  - une procédure doit prévoir la manière dont sont effectuées les sauvegardes (données concernées, fréquence, identification de la personne devant lancer les sauvegardes, support à utiliser, contrôles nécessaires),
  - les sauvegardes doivent être conservées dans des locaux sûrs (exemples : coffres ignifugés et fermés à clé) avec des sauvegardes en double dont un exemplaire doit être conservé en dehors des locaux de la société pour éviter que les deux exemplaires

soient détruits en même temps en cas de sinistre. Possibilité de faire appel à des prestataires externes pour la conservation des sauvegardes,
  - la reprise des données doit être testée régulièrement,
- plan de secours : plusieurs types de solutions de secours sont envisageables :
  - matériel en double,
  - site de repli (concerne essentiellement aujourd'hui les institutions financières, banques, salles de marché…, qui ne peuvent se permettre une indisponibilité de leur système d'information),
  - plan de reprise d'activité en cas de sinistre ou d'indisponibilité du système d'information pendant une longue période,
  - réflexion sur le temps d'indisponibilité critique pour l'activité de l'entreprise et les actions à mettre en œuvre en cas d'indisponibilité longue,
  - procédures de reprise manuelle des opérations.

L'incidence des modalités de la gestion des sauvegardes sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Procédure de sauvegarde	Une procédure de sauvegarde est rédigée et mise à jour. Elle détaille les supports utilisés, le rythme des sauvegardes, les acteurs impliqués dans le processus.	Une procédure est appliquée mais n'a pas été formalisée. *Risque que la procédure ne soit pas correctement appliquée et que la sauvegarde ne soit pas exhaustive.*	Aucune procédure de sauvegarde n'est appliquée dans l'entreprise. *Risque de pertes de données en cas d'incident dans le système d'information.*
Modalités de sauvegarde	Une sauvegarde quotidienne des données sensibles est effectuée. Les supports sont conservés à l'extérieur de la société dans un coffre ignifugé, les états d'exécution sont revus après chaque opération de sauvegarde.	Une sauvegarde quotidienne est effectuée, des tests de reprise des données sont menés par sondage mais les états d'exécution ne sont pas analysés. *Risque que la sauvegarde ne soit pas exhaustive et que des anomalies survenant lors de la sauvegarde ne soient pas décelées.*	Les sauvegardes ne sont pas effectuées régulièrement et les supports ne sont pas testés. *Risque que la sauvegarde ne soit pas exhaustive et que les données sauvegardées ne soient pas toutes récupérables.*
Plan de secours	Un contrat a été passé avec une société spécialisée dans les plans de secours pour une prestation de site de secours ou détention de matériel en double en cas de panne. Un plan de reprise d'activité est formalisé avec les rôles des différents acteurs et les matériels à remettre en marche en priorité. Le plan est régulièrement testé et est opérationnel.	Une réflexion a été menée pour identifier les données les plus sensibles et les parties du système d'information sans lesquelles l'entreprise ne peut plus exercer son activité. Toutefois, aucun plan formalisé de reprise d'activité en cas d'incident n'a été rédigé. *Risque que la mise en place du plan de secours soit désordonnée et que les différents acteurs ne soient pas prévenus de leur rôle en cas d'incident.*	Aucune réflexion n'a été menée au niveau du plan de secours. *Risque d'indisponibilité longue du système en cas d'incident : d'où des difficultés à assurer la poursuite des activités de l'entreprise et un risque de pertes financières et de données.*

Résultat

L'existence et l'efficacité des procédures de sauvegarde et l'éventuelle conception d'un plan de secours augmentent considérablement la capacité de l'entreprise à assurer son activité en cas de sinistre.
Plus l'entreprise est profondément dépendante de son informatique pour la gestion de son activité, plus l'existence de procédures de sauvegarde et d'un plan de secours est critique.

Exemple

Une entreprise de ventes par Internet a subi une inondation causant la perte de ses serveurs informatiques. Le service en ligne est interrompu : les données contenues dans le système sont indisponibles et les ventes sont impossibles pendant tout le temps d'indisponibilité des serveurs. Cela peut entraîner une perte de chiffre d'affaires importante et une perte de clientèle (produits commandés non livrés, commandes impossibles à effectuer dans l'immédiat et délais de remise en marche importants avant la reprise des activités). Si l'indisponibilité est longue, l'absence de plan de reprise d'activité peut entraîner la disparition de l'entreprise.
Un plan de reprise d'activité doit définir les postes clés et les outils informatiques à remettre en marche en priorité de manière à assurer un service clientèle minimum dans toutes les situations.

B. Comment est définie et mise en œuvre la sécurité logique ?

Objectif

La sécurité logique permet de contrôler les risques d'accès aux données par des personnes non autorisées (internes ou externes), ainsi que les risques d'altération des données (notamment par des virus). L'étude de la sécurité logique a pour objectif de vérifier que l'entreprise a mis en place un dispositif adapté à la prévention de ces risques.

Travaux à réaliser

L'étude consiste à :

- vérifier qu'une politique de sécurité logique a été mise en place par l'entreprise :
  - antivirus à jour,
  - protection contre les attaques externes,
- vérifier la politique des habilitations :
  - définition des profils utilisateurs en adéquation avec les fonctions occupées,
  - utilisation d'Internet/messagerie,
  - surveillance de l'accès aux données sensibles,
- analyser les opérations de sensibilisation du personnel à la sécurité logique :
  - existence d'une charte de bonne utilisation du système d'information signée par les utilisateurs,
  - courriels de sensibilisation.

Modalités pratiques

L'étude peut s'appuyer :

- sur l'analyse des documents suivants :
  - architecture technique du réseau,
  - plan de sécurité,
  - charte de sécurité à destination de l'ensemble du personnel,
  - liste des profils et des habilitations par application,
- sur les entretiens avec les personnes suivantes :
  - responsable informatique,
  - responsable de sécurité,
  - responsable de l'exploitation.

L'incidence des modalités de mise en œuvre de la sécurité logique sur le risque inhérent peut s'apprécier à partir des éléments suivants :

- gestion des habilitations, mots de passe, profils d'utilisateurs, authentification… : la gestion des habilitations doit définir précisément les données auxquelles a accès chaque utilisateur selon son poste et sa fonction. Les mots de passe et les procédures d'authentification doivent également permettre d'identifier les personnes se connectant ou ayant créé ou envoyé un message (signature électronique),
- accès à Internet, messagerie, utilisation de disquettes : ces trois outils doivent faire l'objet d'une utilisation explicite, certains sites peuvent être interdits, les données téléchargées peuvent être suivies, les messageries peuvent être contrôlées (après en avoir averti les utilisateurs),
- antivirus à jour : des virus nouveaux apparaissent régulièrement, les éditeurs d'antivirus suivent ces évolutions et mettent à jour les versions de leurs applications. Une mise à jour automatique à chaque connexion permet de s'assurer que la dernière version de l'antivirus est bien installée sur tous les postes en activité,
- pare-feu, suivi des connexions (existence et exploitation) : les règles de filtrage des pare-feu permettent d'interdire certains types de flux. Les suivis de connexion permettent de détecter les tentatives d'intrusion (plusieurs tentatives infructueuses d'accès au réseau sur différents ports à la suite).

L'incidence des modalités de mise en œuvre de la sécurité logique sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Gestion des habilitations / profils utilisateurs	Chaque utilisateur dispose d'un compte avec les droits d'accès nécessaires à sa fonction. Les habilitations sont créées lors de l'entrée du salarié selon sa fonction et désactivées lors de sa sortie. Elles sont régulièrement revues afin qu'aucun compte non utilisé ne soit encore actif.	Des identifiants communs existent au sein de l'entreprise. Seuls deux profils existent : administrateur / utilisateur. *L'identification de l'utilisateur ayant effectué des opérations sous un compte commun est impossible.* *Certains utilisateurs auront des droits trop étendus par rapport à la fonction occupée.* Les entrées/sorties de	L'entreprise ne gère pas de profils différents et ne dispose pas d'une politique de mot de passe. *Risque que des utilisateurs aient des droits illimités alors qu'ils ne doivent pas en avoir l'usage dans le cadre de leur fonction.* Des identifiants communs sont utilisés par plusieurs utilisateurs et aucun profil différent n'a été créé. *Risque que l'identification de la*

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
		personnel ne sont pas communiquées à l'administrateur. *Risque que des comptes d'utilisateurs ayant quitté l'entreprise soient encore actifs et représentent des points d'accès possibles au réseau pour des attaques logiques provenant de l'extérieur.*	*personne ayant effectué des opérations sous un compte commun soit impossible.*
Gestion des mots de passe	Des notes de sensibilisation sont envoyées régulièrement au personnel concernant la gestion des mots de passe. Le système impose un nombre minimum de caractères pour les mots de passe, ainsi qu'un changement régulier aux utilisateurs.	Les mots de passe ne comportent pas de blocage sur leur longueur lors de leur création et ne sont pas changés régulièrement. *Risque que les mots de passe puissent être découverts facilement et que des personnes non autorisées aient accès au réseau de l'entreprise.*	Des mots de passe génériques ou mots de passe faciles à deviner ou identiques à l'identifiant existent pour des comptes utilisateurs ayant des droits étendus. *Risque que les mots de passe puissent être découverts facilement et que des personnes non autorisées aient les droits administrateurs sur le réseau de l'entreprise.*
Utilisation d'Internet / messagerie	L'accès à Internet est contrôlé par un pare-feu (firewall) et limité à quelques postes dans l'entreprise. Le pare-feu a fait l'objet d'un paramétrage. Une charte décrit les modalités d'utilisation de ces outils dans le cadre professionnel.	Aucune sensibilisation à l'utilisation d'Internet et de la messagerie n'a été menée auprès du personnel, mais ces outils ne sont accessibles que de quelques postes spécifiques. *Risque limité d'importation de virus, de visites de sites non autorisés, d'utilisation des outils à des fins personnelles.*	Tous les postes disposent d'une connexion Internet et d'une messagerie mais aucune sensibilisation à leur utilisation n'a été menée auprès du personnel. *Risque élevé d'importation de virus, de visites de sites non autorisés, d'utilisation des outils à des fins personnelles.*
Antivirus	L'entreprise dispose d'un antivirus mis à jour en ligne quotidiennement, installé sur tous les postes et ne pouvant être désactivé par l'utilisateur.	L'antivirus dont dispose l'entreprise n'est mis à jour qu'une fois par mois. *Risque de contamination du réseau par des virus nouveaux.*	Des postes de travail avec lecteurs de disquette ou CD-ROM et accès à Internet ne disposent d'aucun antivirus. *Risque élevé d'importation de virus et de contamination du réseau.*
Protection du réseau	Le réseau est protégé de l'extérieur par un pare-feu (firewall) et les accès utilisateurs font l'objet d'un suivi.	Le réseau est relié à Internet, les flux entrants et sortants sont répertoriés, mais aucun pare-feu n'en assure la protection. *Risque d'attaques logiques provenant d'Internet.*	L'entreprise détient des données sensibles et aucun flux entrant ou sortant du réseau n'est répertorié : les éventuelles attaques dont l'entreprise pourrait être la cible ne peuvent pas être détectées. *Risque d'attaques*

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
			logiques provenant d'Internet ne pouvant être identifiées.
Sensibilisation des utilisateurs	Une charte de bonne utilisation du système d'information est distribuée à l'ensemble des utilisateurs et doit être signée par chacun. Des courriels de sensibilisation sont régulièrement envoyés à tous sur la gestion des mots de passe, la sécurité logique. L'encadrement intermédiaire s'assure du relais de l'information.	Une charte de bonne utilisation du système d'information existe et est remise au personnel à son entrée dans la société : toutefois elle n'est pas à retourner signée à la direction. De même il n'existe pas de preuve que les courriels ou notes internes de sensibilisation ont été lus par les destinataires. *Risque que les utilisateurs n'aient pas lu la charte et ne se sentent pas impliqués dans ce processus.*	Aucune opération de sensibilisation aux problématiques de sécurité logique et/ou aucune formation n'est dispensée aux utilisateurs. *Risque que le personnel effectue des opérations pouvant poser des problèmes de sécurité (échanges de mots de passe, antivirus non mis à jour…).*

Résultat

L'étude des éléments précédents permet d'appréhender la qualité de la politique de sécurité logique et éventuellement de mettre en évidence l'incidence d'une mauvaise séparation de fonctions sur le risque inhérent. Elle peut parfois indiquer des possibilités de fraudes, à partir de tests sur les accès non autorisés au système d'information.

Exemples

Certaines sociétés d'édition ont perdu une partie de leur base documentaire d'images suite à l'irruption d'un virus détruisant les données. Les virus proviennent en grande partie d'Internet et des pièces jointes reçues par messages électroniques.

Une personne ayant un accès illimité au système d'information de l'entreprise peut, si aucune procédure de contrôle n'est mise en œuvre, détourner des sommes, verser des salaires fictifs, modifier les quantités en stocks pour qu'un vol passe inaperçu…

Si les salariés ne sont pas sensibilisés à la sécurité logique informatique, il n'est pas rare que les utilisateurs se communiquent leurs mots de passe, choisissent des mots de passe faciles à deviner ou les écrivent sur un document récapitulatif pour pouvoir avoir accès aux données de tous en cas d'absence. Tout utilisateur peut alors, à partir d'un tel document, accéder à l'ensemble des données de l'entreprise et se trouver à l'origine d'erreurs ou de fraudes.

Si le réseau est connecté à Internet et n'est pas protégé, il peut faire l'objet d'une attaque logique : récupération des données par des concurrents, mise hors service du système (déni de service).

C. La sécurité physique est-elle satisfaisante ?

Objectif

Etudier la gestion de la sécurité physique pour déterminer son incidence sur le risque inhérent, en cherchant à identifier s'il existe :

- un risque de destruction physique des outils informatiques,
- le risque qu'une personne extérieure puisse s'introduire sans autorisation dans les locaux de la société afin d'accéder au système d'information (programmes et données).

Un niveau de sécurité insuffisant peut entraîner, en cas de sinistre, une indisponibilité plus ou moins importante des systèmes d'information.

Travaux à réaliser

L'étude consiste à vérifier :

- les moyens d'accès aux locaux de la société et plus particulièrement ceux abritant les ressources informatiques,
- les moyens de protection dont est dotée l'entreprise pour les types de sinistres suivants :
  - incendie,
  - inondation,
  - coupure de courant/surtension,
  - vol/malveillance,
  - pannes.

Modalités pratiques

L'étude peut s'appuyer :

- sur l'analyse des documents suivants :
  - plan d'accès aux locaux de l'entreprise (localisation de la salle informatique),
  - procédures de sécurité en cas d'incendie,
  - procédures s'appliquant aux visiteurs extérieurs,
  - contrats d'entretien des matériels de sécurité,
- sur les entretiens avec les personnes suivantes :
  - direction de l'entreprise,
  - responsable informatique,
  - responsable de la sécurité,
- sur la visite des locaux et des salles machines pour vérifier que les procédures décrites sont appliquées.

L'incidence de la gestion de la sécurité physique sur le risque inhérent peut s'apprécier à partir des éléments suivants :

- accès aux locaux :
  - existence de badges : sont-ils portés de façon visible par le personnel ? Sont-ils présentés à l'entrée dans les locaux ?
  - gestion des visiteurs : tous les visiteurs doivent être enregistrés et accompagnés dès leur entrée dans les locaux jusqu'à leur sortie,
  - existence de portillons, sas, digicodes,
  - portes des salles machines fermées à clé,
- systèmes anti-incendie :

  - extincteurs automatiques,
  - armoires ignifugées,
  - …,
- existence d'onduleurs permettant le fonctionnement du système d'information en cas de coupure de courant.

L'incidence de la gestion de la sécurité physique sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Moyens d'accès aux locaux	Les locaux sont surveillés, un badge est nécessaire pour y entrer, les visiteurs doivent passer à l'accueil et sont accompagnés pendant la durée de leur présence dans les locaux de l'entreprise, les salles machines sont sécurisées et interdites aux personnes extérieures à la société.	L'entreprise ne dispose pas de sas ou de portillon de sécurité pour accéder à ses locaux. Les visiteurs ne sont pas systématiquement raccompagnés jusqu'à la sortie et aucune pièce d'identité ne leur est demandée à leur entrée, mais les salles machines disposent de digicodes. *Risque que des personnes extérieures à l'entreprise puissent accéder dans les locaux librement.*	Toute personne peut accéder aux locaux de l'entreprise sans se présenter à l'accueil et y circuler librement. Les locaux des salles machines ne sont pas fermés et ne sont pas surveillés. En dehors des heures de travail, les locaux ne présentent pas de dispositifs antivol. *Risque que des personnes puissent librement accéder aux salles machines de l'entreprise.*
Protection incendie	L'entreprise dispose de détecteurs de fumée, d'armoires ignifugées et d'extincteurs. Les salles machines n'abritent pas les consommables et les fournitures.	L'entreprise respecte les réglementations en vigueur de protection incendie, mais ne dispose pas de dispositifs supplémentaires. *Risque de dégâts importants en cas d'incendie.*	L'entreprise ne respecte pas la réglementation en terme de protection incendie. *Risque de pénalités en cas de vérification et risque de dégâts importants en cas d'incendie.*
Protection électrique	L'entreprise dispose d'onduleurs permettant d'éviter des dégâts suite à des coupures de courants ou des variations de tension.	L'entreprise dispose d'onduleurs sur les serveurs les plus critiques. En revanche, les postes de travail n'en sont pas dotés. *Risque de perte de données en cas de coupure de courant.*	L'entreprise ne dispose d'aucune protection contre les variations de tension électrique. *Risque de pertes de données et de matériel en cas d'incidents électriques.*

Résultat

A la suite de ces analyses, des recommandations pourront être formulées pour permettre à l'entreprise de renforcer son niveau de sécurité.

Exemple

Dans des sociétés de petite taille, il n'existe pas toujours de salle machine dédiée au matériel informatique. Les serveurs et autres machines côtoient les photocopieurs (risque d'incendie lié à une feuille bloquée qui s'embrase) et sont situés dans un lieu de passage très fréquenté (risque de malveillance ou d'incident).
Le risque de survenance d'un incident est alors important. Parfois il suffit d'interroger le responsable informatique ou les utilisateurs sur la fréquence et la nature des pannes intervenues dans l'année pour se rendre compte des dangers et qualifier, voire chiffrer le risque.
Si l'entrée dans les salles machines est libre, un employé en conflit avec la direction, ou des personnes malveillantes, peut pénétrer dans les locaux et occasionner des dégâts (destruction de matériel, introduction de virus dans le système, incendie…), pouvant mettre en péril le bon fonctionnement de l'entreprise.

2.1.4. La gestion des projets informatiques

Objectif

Etudier les modalités de gestion des projets informatiques pour déterminer leur incidence sur le risque inhérent. L'utilisation d'une méthodologie est indispensable à tout projet informatique car elle permet à l'entreprise de limiter les retards et les surcoûts liés à la mise en place d'une nouvelle application.

Lorsque le projet informatique représente un investissement significatif, ou lorsqu'il peut avoir une incidence sur le système comptable, il est pertinent d'apprécier l'existence et l'efficience des procédures de gestion de projet au regard des risques financiers généralement encourus ou des conséquences possibles sur les conditions d'établissement des comptes. Dans les autres cas, une telle appréciation n'est pas forcément nécessaire.

Travaux à réaliser

L'étude consiste à :
- vérifier l'existence d'un processus adéquat de gestion de projet :
  - existence d'une équipe projet et d'une maîtrise d'ouvrage pour chacun des projets,
  - découpage des projets en phases,
  - respect et mise en œuvre de chacune des phases,
  - planification de chaque phase,
- vérifier l'existence d'un niveau suffisant de documentation des projets,
- apprécier le degré d'implication de la direction dans la gestion des projets.

Modalités pratiques

L'étude peut s'appuyer :
- sur l'analyse des documents suivants :
  - calendrier des phases des projets en cours,
  - comptes-rendus de réunions de comité de pilotage / suivis d'avancement,
  - documentation des projets touchant à l'informatique (cahier des charges / plan d'assurance qualité …),
  - fiches de tests / fiches de recette,
- sur les entretiens avec les personnes suivantes :
  - direction de l'entreprise,

- responsable informatique,
- chefs des projets en cours,
- maîtrise d'œuvre/maîtrise d'ouvrage d'applications en cours d'élaboration,
- responsable qualité.

L'incidence des modalités de gestion des projets informatiques sur le risque inhérent peut s'apprécier à partir des éléments suivants :

- définition d'une équipe projet :
  - désignation d'un chef de projet,
  - définition d'une maîtrise d'ouvrage et d'une maîtrise d'œuvre distinctes,
  - affectation de ressources dédiées au projet,
  - implication des directions métiers (désignation de responsables),
- définition d'un plan d'assurance qualité, précisant les rôles et responsabilités de chacun,
- implication de la direction dans l'avancement des projets :
  - fréquence des réunions faisant intervenir la direction (comité opérationnel, comité de direction),
  - fréquence des comptes-rendus d'avancement faits à la direction,
- utilisation d'outils de suivi de projet :
  - outils de planification et de suivi d'avancement des tâches,
  - comptes-rendus de réunion,
  - tableaux de bord, outils de pilotage,
  - outils de suivi du budget,
- planification du projet en phases :
  - structuration du projet en plusieurs phases : conception (étude préalable, analyse, appel d'offres), développement (conception détaillée, réalisation, recette de l'application), déploiement,
  - identification de tâches / sous-tâches avec dates d'achèvement,
  - fixation de points intermédiaires,
  - planification de réunions régulières pour suivre l'évolution du projet,
- documentation du projet :
  - documentation tenue à jour,
  - documentation disponible et complète.

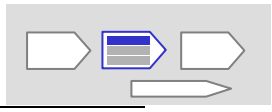
L'incidence des modalités de gestion des projets informatiques sur le risque inhérent peut être schématisée de la manière suivante, en fonction des circonstances rencontrées :

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
Equipe projet	La direction a désigné un chef de projet, une équipe projet, et a fixé le pourcentage de leur temps qui doit être dédié au projet.	Un chef de projet et une équipe ont été désignés mais leur emploi du temps n'a pas été modifié en conséquence. *Risque que l'équipe désignée n'ait pas le temps nécessaire à consacrer au projet : risque de dépassement des délais.*	Aucune équipe n'a été désignée formellement ou une équipe a été désignée, mais plusieurs responsables sont concernés par le projet sans qu'il y ait un véritable chef de projet. *Risque que le projet soit mal piloté : risque de dépassement des délais et des budgets.*
Découpage du projet en phases	Le projet est découpé en tâches et sous-tâches (rédaction d'un cahier des charges / spécifications /	Les phases de conception (cahier des charges / spécifications) sont réduites au profit de la	Le projet est découpé en phases trop longues, aucun point d'avancement n'est

	Incidence sur le risque inhérent		
	Faible	**Modérée**	**Elevée**
	réalisation / recette / déploiement), des points intermédiaires sont fixés, des réunions d'avancement ont lieu régulièrement.	phase de réalisation. *Risque que le projet ne soit pas adapté aux besoins, que des fonctionnalités aient été oubliées lors de la conception et que ces points soient à intégrer tardivement : risque de dépassement des délais et des budgets.*	effectué entre ces étapes. *Risque de retard de calendrier dans les tâches intermédiaires : risque de dépassement des délais et des budgets.*
Niveau de documentation	Les comptes-rendus des réunions d'avancement sont rédigés et conservés. Chaque étape a fait l'objet de documents décrivant les tâches effectuées et leurs conclusions (comptes-rendus de tests, fiches de recette, cahier des charges…).	La documentation existe mais n'a pas été centralisée, elle n'est pas disponible facilement. *Risque de manque de traçabilité sur les différentes phases du projet.*	Aucune documentation n'a été conservée. *Risque de manque de traçabilité sur les différentes phases du projet : aucun moyen de mettre en évidence les tâches effectuées au cours du projet.*
Degré d'implication de la direction dans les projets	La direction a communication de l'avancement du projet sous forme de comptes-rendus réguliers*, en rencontrant le chef de projet ou en participant aux réunions d'avancement. * A relativiser en fonction de la taille de l'entreprise.	La direction a communication de l'avancement par des comptes-rendus réguliers, mais ne participe pas aux réunions de projet. *Risque de manque de responsabilisation de la direction dans le projet et de manque de pilotage.*	La direction délègue son pouvoir de décision au responsable informatique. La direction n'intervient dans le projet que sur sollicitation du responsable informatique. *Risque d'inadéquation de la solution aux besoins des utilisateurs et de non conformité par rapport aux objectifs de la direction.*

Résultat

De la qualité de la méthodologie et du suivi de projet dépend sa réussite. Si les responsabilités sont mal définies, si la direction et les utilisateurs ne sont pas impliqués, un projet a toutes les chances de ne pas aboutir dans les délais et d'entraîner des dépassements de budget qui pourraient mettre l'entreprise en difficulté.
Un projet informatique, dès lors qu'il est significatif financièrement, doit être mené dans le respect des « règles de l'art ». Le commissaire aux comptes pourra sensibiliser les dirigeants sur les risques pesant sur la maîtrise des coûts et la désorganisation du système d'information si une méthodologie de gestion de projet n'est pas respectée. Il ne se prononce pas sur la gestion du projet par l'entreprise, mais il intègre dans sa démarche de travail les conséquences de l'absence, ou du non respect, d'une méthodologie.



Exemple

Une petite et moyenne entreprise, filiale d'un grand groupe, veut mettre en place un progiciel de gestion intégré. Dans un premier temps, une organisation de projet précise a été mise en place. Les chefs de projet et principaux acteurs du projet faisaient partie de la société mère détenant l'entreprise. Quelques mois plus tard, celle-ci a été revendue à un autre groupe, alors qu'elle était en pleine phase de conception de son nouveau système d'information, or aucun responsable appartenant à l'entreprise elle-même n'avait été désigné officiellement responsable du projet.

Après plusieurs années de développement, la solution proposée ne correspondait pas véritablement aux besoins des utilisateurs, ces derniers n'ayant été que faiblement impliqués. Le projet avait coûté le triple du budget initial, avait pris deux fois plus de temps que prévu. L'entreprise était devenue complètement dépendante de ses prestataires et envisageait d'abandonner ce nouveau système d'information au profit d'une autre application plus adaptée aux besoins des utilisateurs. Le nouveau groupe sera contraint de supporter une partie des coûts résultant d'une absence de gestion de projet et qui n'avaient pas été initialement intégrés dans l'évaluation de la PME, au moment de son achat.

2.2. Incidence de l'environnement informatique sur le risque lié au contrôle

L'incidence de l'environnement informatique sur le risque lié au contrôle est appréciée à travers l'étude des processus et des applications jouant un rôle significatif direct ou indirect dans la production des comptes de l'entreprise.

L'identification des contrôles à effectuer est fonction des résultats obtenus dans la phase « Orientation et planification de la mission » et « Incidence de l'environnement informatique sur le risque inhérent ».

L'étude des processus et des applications informatiques permet d'éviter l'effet « boîte noire » consistant à ne voir le système d'information que comme un point d'entrée et de sortie de données, sans connaissance des traitements effectués. Elle doit être menée dans l'objectif de formuler une opinion sur les comptes et de répondre aux obligations légales et professionnelles associées à la mission du commissaire aux comptes.

La fiabilité des contrôles applicatifs mis en place par l'entreprise permet d'alléger les contrôles sur les comptes en apportant une assurance suffisante sur la fiabilité des données présentes dans le système d'information. En cas d'anomalies décelées au niveau des contrôles applicatifs, des contrôles substantifs plus élaborés seront nécessaires, avec ou sans recours à des techniques d'audit assistées par ordinateur.

2.2.1. Généralités sur les contrôles applicatifs

A. Les différents types de contrôles

Il existe deux types de contrôles :
- les contrôles programmés : contrôles effectués automatiquement par une application,
- les contrôles manuels : contrôles effectués par l'utilisateur pour compléter les contrôles programmés.

Ces deux types de contrôles peuvent être préventifs ou de détection :
- les contrôles préventifs sont des contrôles qui sont effectués « a priori », c'est-à-dire avant d'effectuer toute action dans le système. Exemple : identification / authentification par un mot de passe,
- les contrôles de détection sont des contrôles effectués « a posteriori » et qui permettent de déterminer si une anomalie s'est produite. Exemple : état des tentatives d'accès non autorisées.

Les contrôles peuvent être des contrôles bloquants, empêchant l'utilisateur d'aller plus loin si le résultat du contrôle est négatif, ou simplement des alertes qui ont pour objectif d'informer du résultat du contrôle.

Seuls les contrôles programmés seront présentés ci-après, les contrôles manuels faisant l'objet des vérifications habituelles de la part du commissaire aux comptes.

B. Les contrôles programmés

Les contrôles programmés sont les contrôles effectués automatiquement par les programmes aux différents stades du traitement de l'information.
On distingue 4 types de contrôles programmés :
- les contrôles d'accès à l'application,

- les contrôles à la saisie des données,
- les contrôles des traitements,
- les contrôles des sorties.

1) Les contrôles d'accès à l'application

Les contrôles d'accès à l'application ont pour objectifs la vérification de la protection des informations et la confidentialité de celles-ci.
Ils sont nécessaires pour :

- interdire l'utilisation de l'application à toute personne non autorisée,
- accorder le droit à certains collaborateurs d'utiliser certaines fonctions de l'application,
- limiter la consultation des données confidentielles à certains utilisateurs autorisés.

Exemple : à chaque compte utilisateur est associé un profil définissant les droits d'accès, de consultation, de mise à jour des données de tout ou partie des fonctionnalités d'une application.

2) Les contrôles à la saisie des données

Il existe deux niveaux différents de validation sur les données entrées :

- le contrôle des champs de saisie ou données élémentaires,
- le contrôle des ensembles de champs.

a) Le contrôle des champs de saisie

Le contrôle d'un champ de saisie concerne uniquement celui-ci et ne comporte pas de rapprochement avec d'autres éléments saisis.

Désignation du contrôle	Explications et exemples
Nature du champ	Numérique, alphabétique, alphanumérique Exemple : une date de naissance est obligatoirement numérique.
Structure	Organisation interne du champ Exemple : Si la date est saisie sous la forme AA MM JJ, la zone MM ne peut être supérieure à 12.
Saisie obligatoire	Le champ est obligatoirement saisi. Exemple : il ne peut être blanc ou nul.
Intervalle ou plage	Le champ doit être compris entre deux valeurs. Exemple : le numéro de facture doit être compris entre 100 000 et 200 000.
Clé de contrôle	Le champ (en général numérique) contient des données et une zone calculée à partir de ces données, dite clé. L'ordinateur recalcule la clé à partir des données. Si la clé calculée par l'ordinateur est différente de la clé saisie, il y a rejet. Exemple : le numéro de Sécurité Sociale.
Appartenance à un ensemble de valeurs prédéfinies	Le champ peut prendre un nombre limité de valeurs. Exemple : Liste de pays.
Appartenance à un fichier maître	La donnée saisie doit appartenir à un fichier de

Désignation du contrôle	Explications et exemples
	référence. Exemple : La dénomination du fournisseur doit appartenir au fichier des fournisseurs.
Double saisie	Une donnée est saisie sous deux formes pour réduire le risque d'erreur. Exemple : Saisie du code client et du nom du client. Il est aussi possible de faire effectuer la même saisie par deux personnes différentes : l'opérateur et le vérificateur.

b) Le contrôle des ensembles de champs

Le contrôle effectué sur un champ prend en compte la valeur d'autres champs. Ces contrôles visent à vérifier la cohérence d'un ensemble de données élémentaires. L'ensemble considéré peut être :

- un lot d'opérations,
- un enregistrement d'un fichier,
- le fichier lui-même.

1. Lot d'opérations

La saisie par lots consiste à réunir des opérations d'une même nature, ou de nature comparable, et à réaliser une saisie groupée de ces opérations. Ce mode de saisie est plus particulièrement utilisé pour les traitements en temps différé.

En cas de contrôle par lots, l'opérateur saisit :

- l'ensemble des opérations constituant le lot,
- un enregistrement de contrôle dont les zones sont obtenues par totalisation des valeurs caractéristiques des opérations.

L'application effectue à nouveau cette totalisation après saisie et compare le total obtenu au total figurant sur l'enregistrement de contrôle.

Les totaux calculés dans un contrôle par lot sont de trois types :

- les totaux significatifs : les zones additionnées contiennent des devises, quantités ou unités. Le total est significatif (exemple : total des montants des chèques d'un lot),
- les totaux non significatifs : les zones additionnées contiennent des valeurs dont le total n'a aucun sens (exemple : addition des numéros de comptes de comptabilité générale dans un lot d'écritures comptables),
- le comptage d'opérations ou de documents : le total représente un nombre d'opérations ou de documents (exemple : nombre de chèques d'un lot).

La technique de contrôle par lots permet essentiellement de détecter :

- des omissions ou des répétitions de saisie d'opérations au sein d'un lot,
- des omissions ou des erreurs à la saisie des zones caractérisant chaque opération.

2. Enregistrement d'un fichier

L'enregistrement est créé dans le fichier à partir de la saisie à l'écran des zones nécessaires et, éventuellement de champs existants dans d'autres fichiers.

Les contrôles appliqués aux enregistrements sont :

Désignation du contrôle	Explications et exemples
Cohérence / Vraisemblance	La valeur d'une zone est comparée à celle d'une autre en vue de détecter les incompatibilités. Exemple : dans une écriture comptable, débit = crédit.
Signe	C'est un cas particulier du contrôle de cohérence. Le signe + ou – du montant est vérifié avec la nature de l'opération.

3. Fichier

Ces contrôles consistent à comparer des valeurs caractéristiques de l'état d'un fichier à des valeurs caractéristiques de l'état de ce fichier à un moment différent ou caractéristiques de l'état d'un autre fichier.
Les explications concernant le contrôle des fichiers se trouvent aux points 2 et 3 du paragraphe ci-dessous « Les contrôles des traitements ».

3) Les contrôles des traitements

Les contrôles des traitements ont pour objectif de vérifier que :
- toutes les données sont traitées,
- aucune donnée ne disparaît ou n'est artificiellement créée,
- les traitements sont réalisés avec les bonnes versions de fichiers,
- les calculs effectués par les traitements sont exacts.

a) Contrôles sur le déroulement des traitements

Différents types de contrôles permettent de suivre le déroulement des traitements pour vérifier que l'application a effectivement traité les données à traiter et que ces données ont été traitées complètement :

1. Contrôles d'enchaînement de programme à programme

Ces contrôles sont essentiellement adaptés au traitement par lots en temps différé. Les programmes successifs de l'application effectuent la totalisation :
- du nombre d'enregistrements traités,
- des montants unitaires.

Les totaux calculés sont rapprochés afin de détecter d'éventuelles erreurs. Ce rapprochement peut être fait de différentes manières :
- l'édition d'un état de contrôle après chaque programme et d'un récapitulatif en fin d'application (pour rapprochement manuel des totaux),
- la vérification automatique par le programme récepteur des totaux transférés par le programme émetteur avec émission possible d'un message d'erreur en cas d'anomalie,

- l'accumulation des totaux dans des compteurs et réalisation automatique des comparaisons en fin d'application avec impression des totaux et des équations de contrôle sur un état final récapitulatif.

2. Contrôles sur les valeurs caractéristiques des fichiers

Ces contrôles consistent à comparer des valeurs caractéristiques de l'état de ce fichier à un moment différent ou caractéristiques de l'état d'un autre fichier.

Exemple : un fichier d'écritures comptables est mis à jour en temps réel par différents utilisateurs. A la fin de chaque journée, le nombre total d'écritures saisies dans le fichier est calculé. Pour vérifier que les écritures saisies ont été correctement traitées, le contrôle suivant est effectué :

- à la saisie, enregistrement dans un compteur du nombre et du total d'écritures saisies par chaque utilisateur,
- lors du traitement de fin de journée, totalisation du nombre et du montant des écritures du jour et rapprochement avec les valeurs figurant dans les compteurs de saisie.

3. Contrôles de la version utilisée et de la structure des fichiers et des bases de données

– Fichiers

Les paramètres à contrôler pour un fichier sont la version utilisée et sa structure.
Le contrôle de la version permet de vérifier qu'on traite un fichier en tenant compte des dernières mises à jour effectuées. Une version est caractérisée par un numéro ou une date.
Le contrôle de la structure vise à vérifier la cohérence interne du fichier. Il existe différents types de contrôles de cohérence et notamment :

- l'existence de plusieurs types d'enregistrements (exemples : enregistrement d'en-tête, enregistrement détail, enregistrement de fin de fichier),
- l'identifiant unique d'un enregistrement (exemple : clé),
- l'égalité entre la somme des valeurs figurant dans certaines zones fixes de certains enregistrements et un total pré-calculé inscrit dans un enregistrement spécifique appelé enregistrement de contrôle.

– Bases de données

Les principes de contrôles de cohérence des fichiers présentés ci-dessus restent applicables aux bases de données. Il convient cependant de distinguer deux types de contrôles de nature différente :

- les contrôles d'intégrité (exemple : clé unique),
- les contrôles applicatifs (exemple : calcul d'un champ à partir d'autres champs).

4. Contrôles de transmission de fichiers

La transmission de fichiers peut intervenir entre deux applications différentes ou entre deux programmes d'une même application. En cas de transmission, il faut pouvoir contrôler que :

- le fichier reçu est le fichier émis par le correspondant,
- l'émetteur envoie la bonne version du fichier,
- le contenu du fichier reçu est identique au contenu envoyé.

Ces contrôles pourront s'effectuer par des contrôles de version et de structure comme définis précédemment.

5. Sondages et contrôles ponctuels

Lorsque les fichiers sont très volumineux, une exploration intégrale du fichier pour comparer deux états successifs peut être impossible. Des contrôles par sondage sont alors réalisés (contrôles manuels).

Exemple : dans le cas d'un fichier de stocks comportant un nombre très important de références, on effectuera des contrôles sur quelques références afin de vérifier que les traitements effectués dans la journée (préparation de commandes, réception de marchandises, etc.) ont été pris en compte correctement dans le fichier des stocks.

b) Contrôles sur l'évaluation des calculs

La vérification de la correcte évaluation d'un calcul peut être réalisée, soit au niveau d'une opération élémentaire, soit au niveau d'un ensemble d'opérations.
Au niveau de la transaction élémentaire, la fiabilité dépend de la qualité des tests réalisés avant la mise en exploitation.
Au niveau d'un ensemble de transactions, les principaux contrôles applicables sont :

- la comparaison d'un total d'opérations valorisées à un total précédent ou à une moyenne de totaux,
- l'extraction et l'édition des valeurs d'exception (valeurs qui dépassent un intervalle défini),
- le rapprochement entre des valeurs reliées logiquement (exemple : Total HT + TVA = Total TTC).

c) Etats de contrôle

Les états de contrôle permettent de vérifier le déroulement normal des programmes et l'intégrité des fichiers ou bases de données.
Exemple : états des rejets du traitement d'intégration des factures.

4) Les contrôles des sorties

Les sorties sont constituées par le résultat des traitements et par la mise en forme de l'information produite. Les contrôles des sorties doivent permettre de vérifier que :

- le système a imprimé tous les états prévus,
- les états sont complets et exacts,
- les états sont correctement transmis aux bons destinataires.

Les contrôles applicables aux traitements sont applicables aux sorties.

2.2.2. Mise en œuvre de l'appréciation du risque lié aux contrôles applicatifs

Objectif

L'appréciation du risque lié aux contrôles applicatifs porte sur les processus et les applications identifiés dans la phase « Orientation et planification de la mission », à partir des assertions sous-tendant l'établissement des comptes :

- existence : actif ou passif existant à une date donnée,
- exhaustivité : ensemble des actifs, des passifs, des opérations ou des événements enregistrés de façon complète et tous faits importants correctement décrits,
- évaluation : valorisation d'un actif ou d'un passif à sa valeur d'inventaire,
- mesure : opération ou événement enregistré à sa valeur de transaction et produits ou charges rattachés à la bonne période,
- rattachement : opération ou événement se rapportant à l'entité et qui s'est produit au cours de la période,
- droits et obligations : actif ou passif se rapportant à l'entité à une date donnée.

Travaux à réaliser

L'appréciation du risque lié aux contrôles applicatifs suit les étapes suivantes :

- la formalisation des processus sous la forme d'un diagramme de flux ou diagramme d'enchaînement de tâches / étapes,
- l'identification des risques théoriques sur la base des assertions sous-tendant l'établissement des comptes et l'évaluation de leur probabilité de survenance,
- l'identification et l'appréciation des contrôles internes (programmés et utilisateurs) mis en œuvre par l'entreprise pour couvrir les risques correspondants,
- l'incidence sur le risque lié au contrôle.

Modalités pratiques

La formalisation et l'étude du processus s'effectuent sur la base des informations déjà collectées lors de la phase « Orientation et planification de la mission » et d'éventuelles réunions de travail complémentaires avec les différents acteurs de l'entreprise intervenant dans le processus concerné, responsable informatique, responsables opérationnels, utilisateurs (voir le paragraphe sur la formalisation des processus dans l'annexe 1).

L'identification des risques théoriques s'effectue en concertation avec les acteurs et en analysant les composantes applicatives intervenant dans le processus :

- les interfaces (flux entrants, flux sortants),
- les référentiels,
- les habilitations,
- les traitements.

Le tableau suivant indique le degré d'importance (***) que joue généralement chaque composante applicative au regard des différentes assertions sous-tendant l'établissement des comptes :

	Interfaces	Référentiels	Habilitations	Traitements
Exhaustivité	***	*	***	*
Existence	**	*	***	*
Evaluation	*	***	***	***

Exemples :

- les habilitations et les interfaces sont les principaux facteurs à considérer en matière d'exhaustivité,
- les traitements concernent essentiellement l'évaluation et dans une moindre mesure l'exhaustivité ou l'existence.

Une composante applicative sera donc étudiée par rapport à l'assertion vérifiée (exhaustivité, existence, évaluation, mesure, rattachement, droits et obligations…).

Dans un deuxième temps, le commissaire aux comptes identifie et apprécie la qualité des contrôles internes mis en œuvre par l'entreprise au niveau de ces assertions. Ces contrôles pourront être des contrôles programmés ou des contrôles utilisateurs.

L'identification et l'appréciation de ces contrôles s'effectuent par :

- des entretiens avec les utilisateurs et les concepteurs,
- la documentation des différentes applications (en complément des éléments obtenus lors des entretiens),
- des tests de procédure,
- l'utilisation de techniques d'audit assistées par ordinateur.

Principaux contrôles à mettre en oeuvre pour apprécier la fiabilité des processus :

- Flux entrants

Vérification de l'existence et de l'efficience des contrôles suivants :

- les opérations entrées dans le système sont autorisées et validées de manière adéquate,
- la saisie est effectuée correctement,
- les données sont enregistrées dans les fichiers adéquats,
- toutes les anomalies font l'objet de rejet pour correction et retraitement.

- Flux sortants

Vérification de l'existence et de l'efficience des contrôles suivants :

- la correcte évaluation et l'exhaustivité des sorties d'informations sont assurées,
- la diffusion des informations respecte les règles de l'entreprise en matière de confidentialité des données.

- Mise à jour des référentiels

Les référentiels constituent les données permanentes utilisées par le système et à ce titre, participent à la correcte appréciation des traitements réalisés au sein des applications.

Vérification de l'existence et de l'efficience des contrôles suivants :

- les procédures de mise à jour des référentiels existent et sont appliquées,
- les mises à jour sont effectuées de manière simultanée sur l'ensemble du système d'information,
- les paramètres ayant un impact significatif sur les comptes au titre de la piste d'audit font l'objet d'un historique.

- Analyse des traitements

Vérification de l'existence et de l'efficience des contrôles suivants :

- les opérations sont correctement traitées par le système (résultats conformes à ceux attendus),
- il n'existe pas de perte, d'addition, de duplication ou de modification non autorisée des données,
- les anomalies sont identifiées et traitées.

Les vérifications précédentes pourront être complétées par une analyse de la séparation des fonctions existant sur le processus en réalisant une revue de la sécurité logique. Il s'agira de vérifier que les habilitations définies dans le(s) application(s) appartenant au processus satisfont à la séparation des fonctions.
Pour ce faire, il peut être nécessaire d'extraire l'ensemble des profils utilisateurs (ensemble des transactions accessibles à l'utilisateur) et de les rapprocher de l'organigramme détaillé de la société.

D'autre part, outre le fait d'aider à l'identification des contrôles automatisés, l'étude de la documentation permettra également d'évaluer le niveau de dépendance de l'entreprise vis-à-vis d'une personne clé ou d'un prestataire.

Résultat attendu

Pour chaque processus analysé, le commissaire aux comptes dispose des éléments lui permettant de déterminer s'il est possible d'évaluer le risque lié au contrôle à un niveau inférieur à élevé et d'en déduire les contrôles substantifs à mener dans la phase « Obtention d'éléments probants ».

Exemple

Un exemple d'analyse de processus est fourni dans l'étude de cas en annexe.

A. Analyse des interfaces

Objectif

Les applications doivent être adaptées à la structure de l'entreprise (volumétrie, type d'activités gérées…) et doivent garantir la disponibilité et l'intégrité des données, de la saisie initiale à la production des états comptables.

Travaux à réaliser

L'étude des applications et la manière dont elles sont interfacées nécessitent :

- d'utiliser et compléter les travaux de la phase de prise de connaissance,
- d'établir une cartographie précise des applications et de leurs interfaces,
- d'analyser les interfaces reliant les applications entre elles :
  - caractéristiques des interfaces (traitement différé / temps réel, manuelles / automatiques, fréquence),
  - fiabilité des interfaces,
  - modalités de retraitement des anomalies identifiées lors des interfaces avec la comptabilité.

Modalités pratiques

L'étude peut s'appuyer :

- sur les documents suivants :
  - travaux réalisés lors de la phase de prise de connaissance,
  - cartographie applicative existante,
  - documentation des applications de l'entreprise,
  - liste de rejets ou d'anomalies de chaque interface,
- sur les entretiens avec les personnes suivantes :
  - responsable informatique,
  - maîtrise d'ouvrage des applications pour obtenir le détail de ses fonctionnalités et notamment des procédures d'interfaces entre applications,
  - principaux responsables métiers, utilisateurs des applications.

Les vérifications concernent les points suivants :

- caractéristiques des interfaces entre les applications de gestion et la comptabilité : les interfaces sont-elles manuelles (saisies, validation manuelle nécessaire) ou automatiques ?
  - les interfaces manuelles présentent plus de risques d'erreurs (erreurs de saisie, opérations oubliées, doubles saisies…) que les interfaces automatiques,
  - dans le cas d'interfaces automatiques, la vigilance doit porter sur l'existence d'états permettant de vérifier la correcte exécution du traitement (comptes-rendus d'anomalies, comptes-rendus d'exécution permettant de comparer les données en entrée et en sortie du traitement de l'interface). Les états doivent être correctement analysés et donner lieu à des corrections appropriées,
- niveau de fiabilité de l'interface : la fiabilité d'une interface s'effectue en étudiant ses conditions de mise en place, de fonctionnement et de mise à jour. A priori, une interface récente et non complètement testée peut présenter des risques importants d'anomalies,
- mode de traitement des anomalies : il s'agit de vérifier la manière dont sont suivies et traitées les anomalies au niveau des interfaces (en particulier, par qui sont traitées les anomalies et avec quelle périodicité), ainsi que la manière dont elles sont retraitées (recyclage, suppression…). Il est important de savoir qui a la responsabilité de la correction des anomalies

constatées lors des interfaces. Si une telle personne n'est pas désignée, il est probable que les anomalies ne seront pas retraitées correctement.

L'incidence des interfaces sur le risque lié au contrôle peut présenter les situations suivantes :

	Incidence sur le risque lié au contrôle		
	Faible	**Modérée**	**Elevée**
Qualité des interfaces	Les interfaces reliant des applications sont automatiques et stabilisées, les états d'anomalies sont régulièrement édités et analysés par une personne désignée et responsable. Des contrôles réguliers permettent de valider la synchronisation des applications de gestion avec le système comptable.	Les interfaces sont automatiques mais récentes. La personne désignée pour faire les corrections n'a pas examiné les états d'anomalies mais les a conservés. *Les anomalies pourront donc être corrigées mais avec du retard (problème de séparation d'exercice). Le volume d'anomalies peut être important et nécessiter l'implication d'une personne à plein temps.*	Les interfaces sont manuelles (risque de non exhaustivité : erreurs de saisie). Les interfaces sont automatiques mais personne n'est responsable de la correction des anomalies. Les états d'anomalies sont supprimés sans avoir été analysés ni traités. *Les informations ou écritures sont peut-être définitivement perdues ou devront être reconstituées manuellement (lorsque cela est possible).*

Résultat

L'étude de la qualité des interfaces peut mettre en évidence un risque élevé en terme d'exhaustivité de l'information comptable. Des contrôles substantifs seront nécessaires dans la phase « Obtention d'éléments probants » pour quantifier les données non prises en compte en comptabilité et demander à l'entreprise de passer des écritures correctrices, en attente des corrections à apporter aux anomalies détectées. Les interfaces devront en effet faire l'objet de modifications pour éviter de passer chaque année des écritures de correction.
Les problèmes d'exhaustivité de données sont le plus souvent dus à l'absence de traitement des fichiers d'anomalies, lesquels contiennent des données qui ne sont pas transférées en comptabilité. Il convient alors de veiller à ce que les corrections ne soient pas directement effectuées dans le module comptable pour ne pas entraîner des doublons lorsque les interfaces seront rétablies (données identiques comptabilisées deux fois : flux normal issu de l'application amont et saisie directe dans l'application comptable).

En outre, la qualité du retraitement des anomalies est représentative du degré de maîtrise du système d'information de l'entreprise. Le commissaire aux comptes pourra formuler un certain nombre de recommandations de façon à sensibiliser l'entreprise sur l'importance du suivi des interfaces et la nécessité de mettre en place des contrôles supervisés par une personne clairement identifiée.

Exemple

Lors de la mise en place d'un nouveau progiciel, il est fréquent que les interfaces connaissent des dysfonctionnements. Les tables permettant d'affecter une écriture comptable à un événement sont mal paramétrées et certains flux peuvent ne pas donner lieu à comptabilisation.
Dans le cas de la mise en place d'un module de gestion des achats dans un progiciel de gestion intégré, une anomalie d'interface explique qu'une partie des factures ne soit pas enregistrée en comptabilité et ne soit pas réglée aux fournisseurs.
Dans un premier temps, le risque concerne l'exhaustivité des achats.
Par la suite, les fournisseurs voyant qu'ils ne sont pas payés relancent les comptables qui ne peuvent pas débloquer le paiement sans enregistrer une facture. Ils saisissent donc une écriture dans le module finance du programme de gestion intégré sans passer par le module de gestion des achats. Le fournisseur est réglé. Mais le problème d'interface finit par être corrigé et les factures précédemment bloquées se déversent en comptabilité. Ces factures sont maintenant comptabilisées deux fois et risquent de faire l'objet d'un double règlement.

B. Analyse des référentiels

Objectifs

Les référentiels constituent les données permanentes du système d'information utilisées dans les traitements (exemple : taux de TVA). Les modifications apportées à ces référentiels doivent être réalisées par des personnes autorisées. Ces modifications doivent être enregistrées et répertoriées par date de manière à préserver la piste d'audit.

Travaux à réaliser

L'étude consiste à :
- étudier les procédures de mise à jour des référentiels et leur application effective,
- s'assurer que les mises à jour sont effectuées sur l'ensemble du système d'information,
- vérifier les habilitations relatives aux référentiels,
- s'assurer que les données ayant un impact sur les états financiers font l'objet d'une conservation et que leurs modifications font l'objet d'un historique.

Modalités pratiques

L'étude peut s'appuyer :
- sur les documents suivants :
  - cartographie applicative,
  - documentation fonctionnelle de l'application,
  - documentation d'exploitation,
  - manuel des procédures,
- sur les entretiens avec les personnes suivantes :
  - gestionnaire des données,
  - principaux responsables opérationnels,
  - responsable des habilitations.

Les vérifications concernent les points suivants :

- duplication de données :
  - étude de la répartition des données constituant les référentiels au sein du système d'information afin d'analyser l'existence d'un risque de non mise à jour simultanée des données,
- mise à jour des référentiels :
  - étude des habilitations relatives aux données du référentiel pour vérifier que seules les personnes autorisées peuvent réaliser des modifications sur ces données. Les procédures relatives aux données du référentiel et les tests correspondants doivent garantir la pertinence des données le constituant,
  - étude des conditions d'historisation des données du référentiel et des possibilités de reprise de données à une date antérieure, permettant également la vérification des obligations réglementaires,
  - tests pour vérifier que les modifications des référentiels ont bien été réalisées sur l'ensemble des applications constituant le système d'information.

L'incidence des référentiels sur le risque lié au contrôle peut présenter les situations suivantes :

	Incidence sur le risque lié au contrôle		
	Faible	**Modérée**	**Elevée**
Fragmentation des référentiels	Les référentiels sont centralisés dans une banque de données. Les données ne sont pas dupliquées.	Les données constituant le référentiel sont stockées dans différentes bases de données. Il existe une procédure pour s'assurer de la mise à jour simultanée des données.	Il existe plusieurs bases de données qui constituent les référentiels du système d'information. Les données ne font pas l'objet d'une mise à jour simultanée.
Mise à jour des référentiels	Il existe une procédure formalisée pour la mise à jour des référentiels. La modification des référentiels est restreinte à certains personnels.	Il n'existe pas de procédure pour la mise à jour des référentiels. Cependant, les habilitations limitent l'accès en modification à certains collaborateurs.	Les habilitations actuelles ne limitent pas l'accès aux fonctionnalités de mise à jour des référentiels.

Résultat

L'incidence des référentiels sur le risque lié au contrôle concerne essentiellement l'assertion « Evaluation ». L'analyse des procédures concernant ces référentiels permet d'apprécier l'exactitude des traitements informatiques.

C. Analyse des habilitations

Objectifs

Les degrés d'habilitations (droits d'accès et profils utilisateurs) doivent être en relation avec le caractère critique des applications et des ressources à protéger. Mais, parallèlement, ces habilitations ne doivent pas présenter trop de contraintes pour les utilisateurs. Ainsi l'objectif va être d'apprécier le niveau de protection d'une application par rapport au niveau souhaitable compte tenu des caractéristiques de l'entreprise.

Travaux à réaliser

L'étude des habilitations consiste à :

- identifier les facteurs qui contribuent à augmenter ou à diminuer le besoin de protection d'une application,
- apprécier globalement ce besoin,
- vérifier que les habilitations mises en place sont adéquates.

Modalités pratiques

L'étude peut s'appuyer :

- sur les documents suivants :
  - travaux réalisés lors de la phase de prise de connaissance,
  - cartographie applicative,
  - inventaire des applications,
  - procédure de sécurité logique,
  - état des droits d'accès pour chaque application (incluant les modalités de gestion des mots de passe),
  - état des profils utilisateurs,
  - définitions des postes,
  - organigramme,
- sur les entretiens avec les personnes suivantes :
  - responsable informatique,
  - responsable « Exploitation Informatique »,
  - responsable des habilitations,
  - utilisateurs des applications.

En effet, il est utile de rencontrer à la fois les personnes qui ont en charge la mise en œuvre technique des habilitations, mais aussi les personnes qui les délivrent, généralement les directions opérationnelles.

Dans l'appréhension du niveau souhaitable d'habilitation d'une application, il est courant de prendre en compte trois éléments principaux :

(1) le nombre d'utilisateurs potentiels de l'application,
(2) la nature de l'application,
(3) la complexité du système d'information.

(1) Le besoin en procédure d'habilitation croît généralement avec le nombre d'utilisateurs potentiels. A titre indicatif, il est possible de distinguer les ordres de grandeur suivants :
   - 1 à 5 utilisateurs : la séparation des tâches entre les utilisateurs est en pratique difficile à mettre en place. Généralement, les contrôles d'accès aux applications (sous un

environnement micro-ordinateur) se font par le biais des identifiants et des mots de passe,
- 10 à 50 utilisateurs : la séparation des tâches est nécessaire, on voit apparaître la notion de profil utilisateur qui vient s'ajouter aux mots de passe (environnement serveur et micro),
- au-delà de 50 utilisateurs : les applications sont exploitées sur serveurs ou système central, nécessitant un module de gestion spécifique.

(2) Pour apprécier le niveau d'habilitation qui doit être associé à l'application, il convient d'analyser :
- le processus assuré par l'application,
- le caractère critique du processus associé à l'application.

(3) Une application utilise plusieurs ressources informatiques (matériel, logiciel, données). Plus les ressources mises en œuvre sont nombreuses, variées et complexes, et plus l'existence d'une gestion des habilitations, traduisant l'organisation des travaux et la séparation des tâches, sera nécessaire.

Ces éléments d'appréciation, obtenus par entretiens, par l'étude de documents, voire par des tests réalisés directement sur l'application, doivent permettre d'apprécier globalement le niveau souhaitable d'habilitation pour une application donnée.

Les vérifications consistent à rapprocher le niveau d'habilitation souhaitable avec le niveau général d'habilitation de l'application, en prenant en compte les éléments suivants :
- la gestion des mots de passe :
  - existence de standards relatifs à la gestion des mots de passe,
  - renouvellement périodique des mots de passe,
  - historisation des mots de passe,
  - contrôle sur la trivialité des mots de passe (longueur, caractères spéciaux…),
  - absence de stockage des mots de passe en clair,
- les procédures et la documentation :
  - existence d'une procédure de création des habilitations,
  - existence d'une procédure de mise à jour des habilitations,
  - existence de définition de poste,
  - application des procédures existantes,
- les profils et comptes utilisateurs :
  - définition adaptée de profil standard,
  - absence de partage de compte utilisateur,
  - blocage du compte utilisateur après un nombre donné de connexions,
  - existence d'un procédé d'authentification / identification des utilisateurs,
  - existence de fonctionnalités pour assurer l'administration des utilisateurs,
  - mise à jour régulière des bases habilitations,
- l'historisation et le suivi :
  - historisation des traitements réalisés par un utilisateur,
  - revue des journaux applicatifs,
  - revue périodique des habilitations.

Résultat

Le niveau d'habilitation souhaitable mis en relation avec le niveau général d'habilitation de l'application permet au commissaire aux comptes d'apprécier l'incidence des habilitations sur le risque lié au contrôle. A partir de cette étude, il pourra formuler un certain nombre de recommandations relatives aux principales habilitations.

Des faiblesses ou anomalies dans la gestion des habilitations peuvent avoir un impact sur l'ensemble des assertions, une mauvaise gestion des habilitations pouvant affecter l'exhaustivité, l'évaluation, l'existence, etc.

D. Analyse des traitements et paramètres

Objectif

L'étude des traitements et paramètres consiste à vérifier que les données entrées dans une application sont correctement traitées par le système et que les résultats obtenus suite au traitement correspondent bien aux résultats attendus :

- les opérations sont correctement traitées par le système (résultats conformes aux résultats attendus),
- il n'existe pas de perte, d'addition, de duplication ou de modifications des données non autorisées,
- les anomalies de traitement sont identifiées et traitées.

A ce titre, il conviendra de distinguer les progiciels des applications spécifiques développées en interne :

- le risque associé aux progiciels est lié au paramétrage qui est mis en place dans l'entreprise pour configurer le progiciel (l'application ayant fait l'objet de tests par l'éditeur au niveau de la fiabilité des traitements),
- le risque associé aux développements spécifiques peut provenir d'une non conformité des traitements aux spécifications fonctionnelles établies avant les développements.

Travaux à réaliser

L'étude des traitements et paramètres consiste à :

- prendre connaissance de la documentation existante afin d'identifier les contrôles programmés,
- identifier les états d'anomalies existants,
- analyser les procédures de traitements des anomalies,
- étudier les procédures de tests mises en place par l'entreprise pour s'assurer de la conformité des résultats obtenus,
- revoir les comptes-rendus de test,
- étudier la satisfaction des utilisateurs et le niveau de fiabilité de l'application par entretien avec les utilisateurs et le personnel de l'exploitation.

Afin de compléter l'étude, il pourra être réalisé des tests sur les traitements en créant un jeu de tests afin de contrôler l'efficacité des contrôles programmés.

Modalités pratiques

L'étude peut s'appuyer :

- sur les documents suivants :
  - documentation fonctionnelle,
  - documentation technique,
  - dossier de tests,
  - comptes-rendus d'exploitation,
  - états d'anomalies,

  - procédure de traitements des anomalies,
- sur les entretiens avec les personnes suivantes :
  - responsable de l'application (chef de projet informatique),
  - responsable exploitation,
  - utilisateurs.

Les vérifications possibles sont les suivantes :
- identification des contrôles programmés et manuels :
  - par l'étude de la documentation fonctionnelle, de la documentation technique et par entretien, détermination des contrôles programmés présents dans l'application,
  - lors de la description du processus, détermination des contrôles manuels qui sont effectués tout au long du flux d'informations,
- gestion des anomalies :
  - l'efficacité des contrôles mis en place au sein de l'application est appréciée par la consultation des états d'anomalies liés à ces contrôles et par l'étude des modalités de traitement des anomalies,
- procédure de tests :
  - l'exactitude des traitements est appréciée par l'existence de tests réalisés avant la mise en production de l'application. En effet, si des tests ont été menés sur l'ensemble des traitements, que ces tests ont été correctement documentés, les risques d'erreurs liées aux traitements seront faibles,
- maîtrise de l'application :
  - par des entretiens, le commissaire aux comptes pourra évaluer la connaissance de l'application par les utilisateurs ou par le personnel en charge de l'exploitation. Il vérifie que l'utilisation de l'application par les utilisateurs est conforme au mode opératoire défini et ne risque pas de provoquer des erreurs dans les traitements,
- analyse des contrôles périodiques :
  - l'étude des contrôles automatisés ou manuels qui sont opérés dans le processus doit être complétée par l'analyse de contrôles périodiques, consistant par exemple à des rapprochements des données de l'application avec une source externe. En effet, ces contrôles peuvent compenser la faiblesse du contrôle interne des traitements. Ces contrôles peuvent consister par exemple à rapprocher la comptabilité auxiliaire de la comptabilité générale.

Si le commissaire aux comptes ne dispose pas d'éléments suffisants pour apprécier la qualité des traitements et paramètres, il pourra compléter ses travaux en créant un jeu de test et demander à l'entreprise de réaliser des tests de l'application selon ce jeu de test ou bien demander à un expert de réaliser une revue de la programmation ou une revue du paramétrage de l'application.

L'incidence des traitements et paramètres sur le risque lié au contrôle peut présenter les situations suivantes :

	Incidence sur le risque lié au contrôle		
	Faible	**Modérée**	**Elevée**
Anomalies	Il existe des états d'anomalies. Les anomalies font l'objet d'un traitement systématique par des utilisateurs désignés.	Les états d'anomalies ne sont pas traités régulièrement mais sont conservés sans limitation de durée.	Il n'existe pas d'états d'anomalies ou bien ces états ne sont pas traités. De plus, ces états ne sont pas systématiquement conservés.
Test (traitement – paramétrage)	L'ensemble des traitements de l'application a fait l'objet de tests. Les résultats, les anomalies rencontrées, les	Des tests ont été réalisés sur les principaux traitements de l'application. Les résultats	Aucun test n'a été réalisé avant la mise en production de l'application.

	Incidence sur le risque lié au contrôle		
	Faible	**Modérée**	**Elevée**
	solutions apportées sont documentés.	de ces tests n'ont pas été formalisés.	
Formation des utilisateurs	Les utilisateurs ont reçu une formation leur permettant d'acquérir une bonne maîtrise de l'application.	Les utilisateurs n'ont pas reçu de formation mais possèdent une bonne connaissance des traitements courants suite à l'utilisation régulière et importante de l'application.	Les utilisateurs n'ont pas pu s'approprier l'application et ne maîtrisent pas les fonctions courantes.

Résultat

L'étude des traitements et paramètres va permettre de mettre en évidence des risques en matière d'évaluation et d'exhaustivité des données traitées dans l'application.

2.3. Synthèse de l'évaluation des risques

Lors de l'évaluation des risques, l'incidence de l'environnement informatique sur le risque inhérent et sur le risque lié au contrôle a été prise en compte et le risque de non détection permet de déterminer les contrôles substantifs à mener dans la phase « Obtention d'éléments probants ».

Il convient de rappeler que le risque le plus important pour le commissaire aux comptes est le risque de non détection. La relation entre les différentes composantes du risque d'audit est présentée dans le tableau suivant, lequel indique comment le risque de non détection peut varier en fonction de l'appréciation du risque inhérent et du risque lié au contrôle.

Les zones grisées correspondent au risque de non détection. Plus le niveau de ce risque est faible, plus les contrôles à mettre en œuvre par le commissaire aux comptes sont importants.

Evaluation par le commissaire aux comptes du risque inhérent	**Evaluation par le commissaire aux comptes du risque lié au contrôle**		
	Elevé	Moyen	Faible
Elevé	*Minimum*	*Faible*	*Moyen*
Moyen	*Faible*	*Moyen*	*Elevé*
Faible	*Moyen*	*Elevé*	*Maximum*

La norme CNCC 2-301 « Evaluation du risque et contrôle interne » précise dans le paragraphe .47 - que « plus le risque inhérent et le risque lié au contrôle sont évalués à un niveau élevé, plus le commissaire aux comptes réunit d'éléments probants provenant de contrôles substantifs. Lorsque ces risques sont évalués à un niveau élevé, le commissaire aux comptes détermine si les contrôles substantifs fournissent des éléments probants suffisants pour réduire le risque de non détection, et donc le risque d'audit à un niveau acceptable faible. Lorsqu'il constate que le risque de non détection concernant une assertion sous-tendant l'évaluation d'un solde de compte ou d'une catégorie d'opérations significatif ne peut être réduit à un niveau acceptable faible, le commissaire aux comptes exprime dans son rapport une opinion avec réserve ou un refus de certifier pour limitation ».

3. OBTENTION D'ELEMENTS PROBANTS

L'obtention d'éléments probants sur les comptes est effectuée sur la base de l'évaluation des risques, afin de pouvoir aboutir à des conclusions fondant l'émission de l'opinion.

Si l'appréciation du contrôle interne est menée tout au long de l'exercice, l'obtention d'éléments probants au moyen de contrôles substantifs intervient dans la période de clôture des comptes.

La norme CNCC 2-302 précise les points suivants dans le paragraphe .12 - : « Les objectifs d'audit restent identiques, que les données comptables soient traitées manuellement ou par informatique. Toutefois, les méthodes de mise en œuvre des procédures d'audit pour réunir des éléments probants peuvent être influencées par le mode de traitement utilisé. Le commissaire aux comptes peut appliquer des procédures d'audit manuelles, des techniques assistées par ordinateur, ou combiner les deux pour rassembler suffisamment d'éléments probants. Toutefois, dans certains systèmes comptables utilisant un ordinateur pour traiter des applications importantes, il peut être difficile, voire impossible, pour le commissaire aux comptes de se procurer certaines données à des fins d'inspection, de vérification ou de confirmation externe sans utiliser l'informatique ».

3.1. Méthodes de mise en œuvre des procédures d'audit

Le commissaire aux comptes, à partir des éléments vérifiés lors de l'évaluation des risques, se concentre sur les risques de niveau modéré ou élevé, afin de déterminer la nature et l'étendue des contrôles substantifs à mener et s'il est pertinent, pour ce faire, de recourir aux techniques d'audit assistées par ordinateur (cf. chapitre 3).

3.2. Lien avec les obligations légales du commissaire aux comptes

Après avoir effectué les contrôles substantifs nécessaires et disposant des éléments probants suffisants et appropriés recherchés, le commissaire aux comptes peut émettre une opinion sur les comptes de l'entreprise. Cette opinion est fonction notamment du caractère significatif des anomalies éventuellement relevées.

Le commissaire aux comptes détermine également l'impact des conclusions de ses travaux sur les autres aspects de la mission, tels que l'information des dirigeants ou de l'organe de direction.

3.2.1. Emission de l'opinion sur les comptes

Les contrôles effectués sur les systèmes comptable et de contrôle interne peuvent mettre en évidence des anomalies (insuffisances ou erreurs) de nature à avoir un impact sur l'opinion du commissaire aux comptes.

Exemples d'anomalies liées aux contrôles applicatifs, identifiées lors de l'évaluation des systèmes comptable et de contrôle interne, qui pourraient avoir une incidence sur l'opinion du commissaire aux comptes :

- opérations ou montants significatifs non transmis par une interface entre deux applications et qui n'ont pas été enregistrés en comptabilité,
- identification d'une anomalie significative lors de l'analyse d'un fichier informatique (provision mal calculée, erreur de valorisation des stocks, …),
- absence ou erreur dans la mise à jour du référentiel d'une application (exemples : ventes, paie),
- absence d'archivage des données et/ou programmes impliquant un risque significatif de taxation d'office en cas de contrôle fiscal (loi sur le contrôle fiscal informatisé),
- absence de procédure de sauvegarde des données et/ou programmes impliquant un risque de perte financière en cas de sinistre majeur (incendie, acte de malveillance, intrusion, …),
- contrôle interne déficient ou absent, au sein d'une application qui gère un processus majeur de l'entreprise,
- mise en évidence d'irrégularités ou d'inexactitudes.

3.2.2. Information des dirigeants ou de l'organe de direction

Une bonne connaissance du contrôle interne, notamment au regard du système d'information, permet de relever des faiblesses ou anomalies qui pourront être communiquées aux personnes constituant le gouvernement d'entreprise, conformément à la norme CNCC 2-107 « Communication sur la mission avec les personnes constituant le gouvernement d'entreprise ».
Dans les sociétés anonymes, les modalités d'information du gouvernement d'entreprise sont définies dans l'article L. 225-237 du Code de commerce.

Les remarques du commissaire aux comptes concernant le système d'information de l'entreprise sont porteuses d'une forte valeur ajoutée qui intéresse les dirigeants. Ces remarques leur permettront de mettre en œuvre des solutions palliatives / correctives, de façon à renforcer le plus rapidement possible la qualité du contrôle interne.

Les principaux risques d'origine informatique résultent essentiellement de l'indisponibilité du système d'information ou de dysfonctionnements majeurs de longue durée d'une application stratégique pour l'entreprise.

A. Indisponibilité des systèmes

La poursuite d'activité d'une entreprise peut être fortement liée à sa capacité à redémarrer son informatique dans des délais très brefs. Le commissaire aux comptes, lors de l'appréciation des risques liés aux contrôles applicatifs, vérifie que l'entreprise a mis en place une procédure de sauvegardes et des sauvegardes effectives de ses systèmes, mais aussi qu'elle a réfléchi à sa capacité à retrouver son fonctionnement normal en cas de sinistre majeur (définition d'un plan de secours).

La pratique de sauvegardes régulières n'est pas une garantie suffisante de la capacité de l'entreprise à pouvoir assurer la poursuite de son activité. D'une part, l'entreprise doit vérifier qu'elle est capable d'exploiter ses sauvegardes (en particulier, lors de changements de matériels) et que les sauvegardes réalisées couvrent l'ensemble des applications, incluant données et programmes. D'autre part, l'entreprise doit identifier la durée pendant laquelle elle peut se passer de son informatique et évaluer le préjudice qu'elle pourrait subir en son absence.

B. Dysfonctionnement important d'une application stratégique

Un dysfonctionnement important d'une application conditionnant une activité majeure de l'entreprise peut avoir une incidence sur la poursuite d'activité. En effet, des anomalies importantes et répétées d'une application peuvent constituer un risque élevé en termes de pertes financières, de dégradation d'image, de pertes de part de marché qui peuvent conduire, dans les cas extrêmes, à la cessation d'activité d'une société.
Cependant, pour que l'incidence sur la continuité d'exploitation soit réelle, il faut, en général, que les dysfonctionnements s'étalent dans le temps et soient répétés. Plus une entreprise réagira rapidement pour les corriger, moins le risque de remise en cause de son activité sera important.

CHAPITRE 2 : LES DOSSIERS THEMATIQUES

1. THEME 1 : L'ORGANISATION DE LA FONCTION INFORMATIQUE DANS L'ENTREPRISE

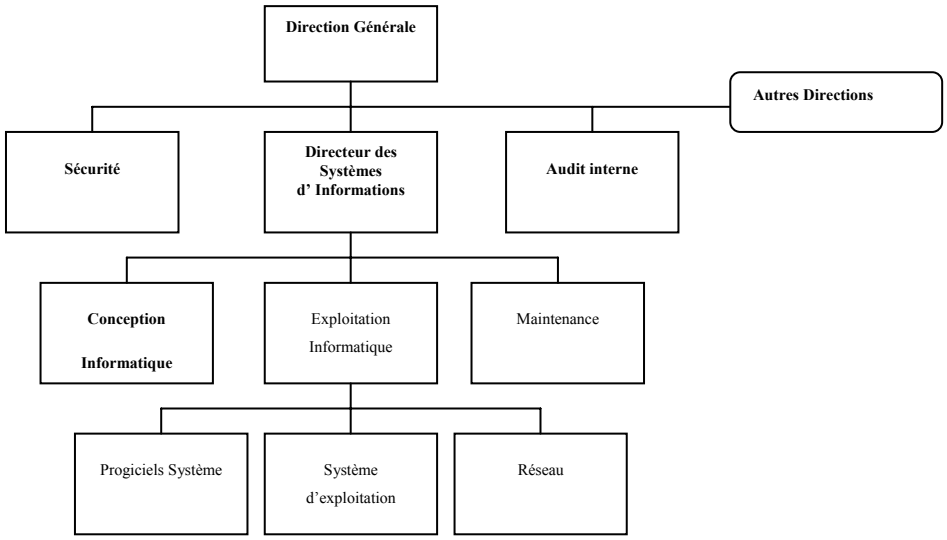
1.1. Organigramme

Le schéma ci-dessous présente les principales fonctions d'une direction informatique dans une entreprise de taille importante et permet :

- d'avoir une vue détaillée des différentes spécialités existant en informatique,
- d'identifier les compétences informatiques couvertes et non couvertes dans l'entreprise.

L'objectif de ce dossier thématique est de mieux appréhender les fonctions informatiques abordées dans le chapitre Méthodologie, au niveau de la « Prise de connaissance de l'informatique dans l'entreprise » et de l'« Incidence de l'informatique sur le risque inhérent ».

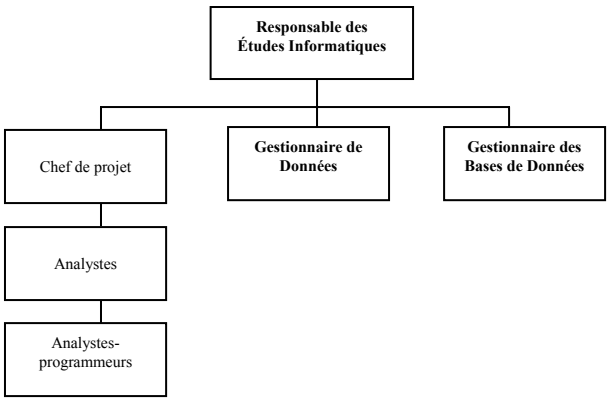
Rattachée traditionnellement à la direction administrative et financière de l'entreprise, la direction informatique est désormais de plus en plus hiérarchiquement rattachée à la direction générale, à qui les choix stratégiques incombent en raison de leur importance.



1.2. Conception informatique

Le service « Conception informatique » (appelé également service « Etudes ») regroupe l'ensemble des fonctions de base (analyse, programmation, contrôle qualité, gestionnaire des données, gestionnaire de la base de données) qui concourent à la mise en place des nouveaux systèmes informatiques. Les Études développent des programmes ou des évolutions fonctionnelles d'après les spécifications des utilisateurs. Après validation (par tests) des utilisateurs, les programmes ou codes sources sont transmis au service « Exploitation informatique », en charge de la mise en œuvre opérationnelle.

Le service comprend généralement un responsable des Études, un chef de projet, des analystes, des analystes-programmeurs, un gestionnaire de données, un gestionnaire des bases de données.



Exemple d'organigramme d'un service « Conception Informatique »

1.3. Exploitation informatique

Le service « Exploitation informatique » regroupe :

- l'ensemble des fonctions nécessaires à la mise en œuvre sécurisée des traitements transactionnels et différés composant les applications informatiques :
  - la sécurité physique et logique, si elle n'est pas assurée par une fonction sécurité indépendante,
  - l'exploitation des applications (traitements différés, sauvegarde, reprise…),
  - l'administration des composants matériels (serveur, réseau…),
  - le suivi et l'optimisation des performances (disponibilité, temps de traitement…),
- la mise en exploitation des applications acquises ou développées par la fonction Études Informatiques.

1.4. Maintenance

Le service « Maintenance » concerne :

- la fonction « Conception », avec la maintenance applicative qui peut être corrective ou évolutive. Dans le premier cas, la maintenance consiste à corriger les programmes sources présents dans l'environnement d'exploitation et dans le second, à y adjoindre des fonctionnalités complémentaires en fonction des demandes des utilisateurs. Elle peut également correspondre à une évolution réglementaire imposant une adaptation des programmes (exemples : passage à l'an 2000, à l'euro…),
- la fonction « Exploitation », avec la maintenance des systèmes et des réseaux qui a pour but d'assurer la continuité de l'activité au quotidien. Elle comprend la maintenance des infrastructures et des systèmes d'exploitation.

1.5. Sécurité

Cette fonction est essentielle dans un environnement informatique dans lequel la protection des données de l'entreprise constitue une nécessité absolue. Un schéma directeur de la sécurité doit être élaboré, comprenant notamment la définition et le suivi des procédures de contrôle d'accès physiques et logiques aux données informatisées.

Cette fonction peut être assurée :

- soit par un service indépendant qui assurera la sécurité de l'ensemble de l'entreprise, y compris du système d'information (protection des actifs, gestion des droits d'accès dans les locaux, protection incendie et inondations…),
- soit par le service « Exploitation Informatique » qui assurera uniquement la sécurité physique et logique du système d'information (applications, systèmes et réseaux).

2. THEME 2 : LES OBLIGATIONS REGLEMENTAIRES

Les entreprises sont soumises pour leurs systèmes d'information à des obligations réglementaires spécifiques. Le commissaire aux comptes devra s'assurer du respect de ces obligations, notamment :

- l'archivage fiscal et le contrôle des comptabilités informatisées,
- la protection des données personnelles,
- la protection des logiciels.

2.1. Archivage fiscal et contrôle des comptabilités informatisées

2.1.1. Objectif

L'archivage fiscal doit permettre à une entreprise de répondre à une demande d'information émanant de l'administration fiscale dans le cadre de la réglementation applicable (article 103 de la loi de finances pour 1990, complétée par la loi du 10 mai 1994 spécifique aux programmes développés par des prestataires).

Les instructions administratives, des 14 octobre 1991 et 24 décembre 1996 commentant ces dispositions, précisent les obligations incombant aux contribuables dont la comptabilité est informatisée et peuvent être résumées comme suit :

- mise à disposition de l'administration fiscale de tout élément d'information ou traitement concourant directement ou indirectement à la formation des résultats comptables ou fiscaux,
- tenue d'une documentation informatique :
  - décrivant le système d'information mis en œuvre au cours de la période vérifiée,
  - explicitant les règles de gestion des données et des fichiers mises en œuvre dans les programmes informatiques et ayant des incidences directes ou indirectes sur la formation des résultats comptables et fiscaux et des déclarations rendues obligatoires par le Code Général des Impôts.

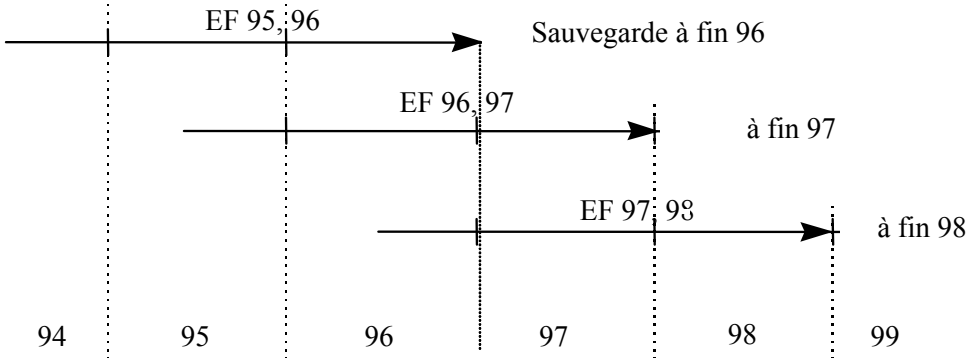
Les informations présentées ci-dessous concernent davantage les bonnes pratiques et les modalités d'application de l'archivage fiscal et du contrôle des comptabilités informatisées, qu'une présentation des textes de référence.

2.1.2. Cahier des charges

A. Plan d'archivage

Ce plan a pour but de répondre aux demandes de traitement que l'administration fiscale pourrait vouloir réaliser dans les domaines vérifiés. La constitution des archives pourra être réalisée, soit à partir des sauvegardes existantes (exemple : arrêtés de stocks), soit à partir des données en ligne.
Il est recommandé d'effectuer une sauvegarde annuelle couvrant plusieurs exercices fiscaux (EF). Ainsi, un même exercice sera sauvegardé sur plusieurs supports.

Dans l'exemple ci-dessous, une sauvegarde couvrant deux ans et demi est effectuée chaque année.



B. Format d'archivage

Le format d'archivage recommandé est un fichier « à plat à organisation séquentielle ».

C. Gestion de l'archivage

Un document appelé « Fiche détaillée de suivi de la constitution des archives » peut synthétiser toutes les informations relatives au support physique d'archivage.

1) Nature des supports

Les éléments à prendre en considération dans le choix du support peuvent être la pérennité, le rapport volumétrie/capacité physique ou la sécurité des supports.

2) Règle d'archivage des supports

Il est préférable que chaque support physique ne concerne qu'une sauvegarde. Cette sauvegarde peut couvrir un ou plusieurs exercices.

3) Identification des supports

L'identification du support est un point important. Les éléments à faire figurer sur le support sont : la date de la sauvegarde, la période concernée, l'exercice couvert, l'application concernée et si possible, les noms physiques des fichiers.

4) Stockage des supports

Les supports sont stockés dans un coffre (ignifugé si possible) et sont placés sous la responsabilité de la direction comptable afin de parer à toute erreur d'utilisation. Un jeu de sauvegardes devra aussi être dupliqué et conservé hors du site ou confié à un prestataire externe qui s'engagera contractuellement à le conserver tant que les données contenues seront susceptibles d'être contrôlées.

2.1.3. Procédures de mise en place du cahier des charges

La réalisation du cahier des charges nécessite la mise en place de contrôles visant à garantir une constitution appropriée des archives. En particulier, un contrôle de transfert des données doit être réalisé lors de chaque écriture de support. Il a pour objectif de s'assurer de l'exhaustivité des données de production qui ont été copiées sur le support.

Une fois l'archive constituée, il est conseillé de communiquer à la direction comptable la première page du contenu du fichier, afin de s'assurer de l'existence et de la pertinence des données sauvegardées sur le support.
Enfin, des tests de relecture par sondage devront être réalisés périodiquement en particulier sur les archives concernant les exercices les plus anciens ouverts à contrôle.

Tableau 1 : TABLEAU DE SUIVI DE LA CONSTITUTION DES ARCHIVES

N° DE SUPPORT	NOM PHYSIQUE DU FICHIER	APPLICATION	DESCRIPTION FONCTIONNELLE	DATE DE CREATION DE LA SAUVEGARDE ORIGINE	EXERCICE COUVERT	PERIODE	CONTROLE EFFECTUE	SUPPORT UTILISE	DATE CREATION ARCHIVE	DATE STOCKAGE ARCHIVE
	XYZ	A	Comptabilité Auxiliaire Client	02/01/99	1998	06/97 => 12/98	↗	DAT 4mm	22/03/99	22/03/99

Tableau 2 : FICHE DÉTAILLEE DE SUIVI DE LA CONSTITUTION DES ARCHIVES

Date Création Archive : Fait par :							
Numéro Support						Type Support	
Synthèse de l'archive							
Nom physique	Descriptif	Applicatif	Exercice	Période	Date origine de l'archive	Contrôle	
						Nb Enreg. Avant	Nb Enreg. Après
Remis le :			Visa :				

2.1.4. Plan de mise en conformité

A. Organiser le plan d'archivage

Compte tenu des conséquences fiscales consécutives à l'absence d'archivage des données du système d'information, il est essentiel qu'une procédure de contrôle périodique des archives soit mise en place, notamment selon le processus suivant :

- les services informatiques supervisent les opérations d'archivage liées aux procédures d'arrêté mensuel,
- ils mettent à jour un document d'inventaire des archives de la période reprenant en particulier les fichiers et supports magnétiques créés,
- ils transmettent ce document à une personne de la direction comptable, qui à tout moment, dispose du détail des archives réalisées et peut juger de l'exhaustivité de celles-ci,
- un responsable du plan d'archivage est désigné au sein de la direction comptable,
- un document de suivi des archives réalisées doit être formalisé.

B. Organiser les arrêtés comptables

Les comptes pouvant être soumis à vérification par l'administration fiscale deviennent définitifs à l'issue de la clôture de toutes les chaînes d'informations qui alimentent directement ou indirectement l'application de comptabilité. Afin d'organiser les arrêtés comptables, il faut :

- transmettre aux informaticiens les dates d'arrêtés des différentes chaînes d'informations définies par le service comptable en liaison avec les services utilisateurs,
- intégrer dans les programmes d'arrêtés mensuels des instructions relatives aux différents fichiers à archiver,
- dissocier les opérations de purge (consistant à vider les bases de données) de l'archivage,
- n'archiver des données que par rapport à des dates d'arrêtés comptables.

C. Assurer l'exhaustivité des archives

1) Les données

Du fait de la limitation de certaines tables ou des temps de réponse du réseau qui deviendraient importants, les opérations consistant à vider les bases de données peuvent être effectuées régulièrement. Il est important que ces opérations soient planifiées et systématiquement précédées d'un contrôle des archivages déjà réalisés, prenant en compte les dates d'arrêtés comptables, avec tests de relecture.

2) Les programmes

Pour l'ensemble des programmes en exploitation, il convient de conserver pour chaque année les versions successives des programmes ayant subi des modifications fonctionnelles.
De plus, un recensement exhaustif des sources disponibles doit être effectué. La procédure de sauvegarde doit inclure les éléments suivants :

- un archivage systématique de tous les programmes présents dans l'environnement de production à la clôture de l'exercice,
- une trace écrite des modifications fonctionnelles significatives :
  - les modifications devant faire l'objet d'une sauvegarde spécifique doivent être décidées conjointement par les utilisateurs et le service informatique,
  - les informations à conserver lors d'une modification de programme sont celles qui permettent de faire le lien entre une règle fonctionnelle et les programmes eux-mêmes. Elles peuvent consister en une fiche de liaison (demande de l'utilisateur), une description détaillée de la règle de calcul adoptée, une liste des programmes modifiés.

D. La documentation

Dans le cadre juridique du contrôle des comptabilités tenues au moyen de systèmes informatisés définis par la loi de finances pour 1990, les demandes de consultation de la documentation des systèmes informatiques pourraient porter sur les informations suivantes :

- règles de calcul utilisées pour l'élaboration des données concourant à la formation du résultat comptable,
- procédures de contrôle de la centralisation des informations en comptabilité,
- procédures de contrôle des accès au système d'information.

Par les instructions des 14 octobre 1991 et 24 décembre 1996, l'administration fiscale précise le champ d'application de la procédure de contrôle des comptabilités informatisées.

Cette procédure couvre non seulement les « informations, données et traitements informatiques qui concourent directement ou indirectement à la formation des résultats comptables et fiscaux », mais elle inclut également la « documentation informatique retraçant les différentes phases du processus de conception, d'exploitation et de maintenance des systèmes informatiques ».

E. Organiser le contrôle des sauvegardes

1) Assurer la lisibilité des sauvegardes

Il est préférable de procéder à un archivage des fichiers sous un format « à plat », ce qui permet leur relecture à partir d'outils de requêtes. Toute la procédure de création des supports doit être systématiquement mise en œuvre afin de maintenir la protection des données archivées.

2) Assurer la pérennité des données

Afin de s'assurer de l'absence de problème de relecture des archives créées (objectif final d'un plan d'archivage) et de leur cohérence avec la comptabilité, le service comptable peut demander périodiquement au service informatique de procéder à des tests de relecture et de totalisation.

F. Organiser les relations avec les tiers (prestataires / éditeurs de progiciels)

La société doit convenir avec ses prestataires de services des dispositions contractuelles garantissant les obligations suivantes :

- la possibilité pour l'administration fiscale d'accéder aux programmes sources,
- la possibilité d'obtenir les données archivées sous forme de fichiers « à plat »,
- l'assistance technique d'un consultant en cas d'intervention de la Brigade de Vérification des Comptabilités Informatisées (BVCI).

G. S'affranchir des contraintes liées aux changements de système

A l'occasion des changements de systèmes informatiques, des modifications de référentiels peuvent être réalisées (pour les références des produits, des comptes, ...). Il est alors nécessaire de conserver une table de correspondance entre l'ancien et le nouveau référentiel, permettant de répondre à une demande de l'administration qui porterait sur une comparaison entre deux exercices utilisant des référentiels différents.

2.1.5. Points de fiscalité

Dans le cadre de la réglementation applicable (article 103 de la loi de finances pour 1990, complétée par la loi du 10 mai 1994), l'administration fiscale, aidée des BVCI, est en droit, en application de l'article L. 47 A du Livre des Procédures Fiscales (LPF), de demander la réalisation de traitements informatiques qu'elle jugerait nécessaires à la conduite des opérations de vérification de comptabilité.

A. Les obligations incombant aux contribuables

Les instructions administratives des 14 octobre 1991 et 24 décembre 1996 ont précisé les obligations incombant aux contribuables dont la comptabilité est informatisée. Elles peuvent être résumées de la façon suivante :

1) Obligations de conservation...

Il s'agit des données, traitées par des applications informatiques, qui concourent à la constitution d'enregistrements comptables ou à la justification d'un événement ou d'une situation transcrite dans les livres, registres, documents, pièces et déclarations contrôlés par l'administration. Le contribuable doit pouvoir reconstituer les soldes à partir des données élémentaires.

2) ...Pendant un certain délai...

Doivent être distingués :
- les documents visés par les droits de communication et de contrôle de l'administration fiscale,
- les données, traitements et documentations, soumis à une obligation de conservation de durée plus réduite.

Ainsi, le délai général de conservation de six ans (art. L 102 B du LPF) s'applique aux livres, registres, documents ou pièces auxquels l'administration a accès pour procéder au contrôle des déclarations et des comptabilités des contribuables astreints à tenir et à présenter des documents comptables.
Pendant ce délai, une modalité spécifique de conservation est prévue (Cf. 2e alinéa de l'article L. 102 B du LPF) pour les documents établis ou reçus sur support informatique qui doivent obligatoirement être conservés sur ce support jusqu'à la fin de la troisième année suivant celle à laquelle elle se rapporte (art. L. 169 du LPF).
A l'issue de ce délai, et jusqu'à l'expiration du délai général de six ans, ces documents pourront être conservés sur le support choisi par le contribuable.
De plus, la législation propre aux comptabilités informatisées impose aux contribuables de conserver pendant ce même délai, sur le support initial (papier ou informatique), la documentation relative aux analyses, à la programmation et à l'exécution des traitements. Les données concernées sont les données élémentaires permettant de reconstituer les agrégats.

3) ...De la documentation

La conservation de la documentation répond à deux objectifs complémentaires :

- un objectif informatique : l'analyse de la documentation doit permettre au vérificateur de connaître et de comprendre le système d'information mis en œuvre au cours de la période soumise au contrôle, y compris l'ensemble des évolutions significatives,
- un objectif fiscal : la documentation doit décrire de façon suffisamment précise et explicite les règles de gestion des données et des fichiers mises en œuvre dans les programmes informatiques et qui ont des incidences directes ou indirectes sur la formation des résultats comptable et fiscal et sur les déclarations rendues obligatoires par le Code Général des Impôts.

Tableau de synthèse

<table>
<tr><th colspan="3" rowspan="2">Informations à conserver</th><th colspan="3">Durée de conservation</th></tr>
<tr><th>3 ans</th><th>6 ans</th><th>10 ans</th></tr>
<tr><td rowspan="4">Informations visées par les droits généraux de communication et de contrôle de l'administration</td><td colspan="2">Livres et registres obligatoires</td><td colspan="3">Sur leur support original</td></tr>
<tr><td rowspan="3">Autres documents ou pièces justificatives</td><td>établis sur support non informatique</td><td colspan="3">Sur tout support</td></tr>
<tr><td>établis sur support informatique</td><td>Sur support informatique</td><td colspan="2">Sur tout support</td></tr>
<tr><td>ouvrant droit à déduction de TVA</td><td colspan="2">Sur leur support original</td><td>Sur tout support</td></tr>
<tr><td rowspan="2">Informations supplémentaires du fait qu'elles ont trait à l'informatique</td><td colspan="2">Autres informations, données ou traitements informatiques non visés ci-dessus, mais concourant directement ou indirectement à la formation des résultats comptables ou fiscaux et à l'élaboration des déclarations rendues obligatoires par le Code Général des Impôts</td><td>Sur support informatique</td><td colspan="2" rowspan="2">Aucune obligation de conservation</td></tr>
<tr><td colspan="2">Documentation informatique</td><td>Sur leur support original</td></tr>
</table>

B. Le contrôle fiscal de la comptabilité informatisée

1) Les modalités de contrôle

L'article L. 47 A du L.P.F. est mis en œuvre à l'initiative des agents de l'administration selon trois modalités de contrôle :

- par des agents de l'administration fiscale sur le matériel de l'entreprise,
- par le contribuable sur le matériel de l'entreprise, sous le contrôle de l'administration,
- par des agents de l'administration fiscale sur du matériel n'appartenant pas au contribuable vérifié.

Selon la nature des traitements demandés, l'entreprise fait connaître par écrit à l'administration la modalité de contrôle retenue. Le choix laissé à l'entreprise ne s'applique pas à la totalité du contrôle, mais à chaque point contrôlé.

2) Le risque de la mise en oeuvre de l'évaluation d'office

L'article L. 74, 2^{e} alinéa du LPF, prévoit que les bases d'imposition sont évaluées d'office en cas d'opposition à la mise en œuvre du contrôle des comptabilités informatisées. L'administration a par ailleurs précisé que cette procédure d'évaluation d'office devait, à son sens, trouver à s'appliquer dans

des situations où le contrôle informatique se révélerait de fait impossible, et notamment dans les hypothèses suivantes :

- le contribuable s'abstient de répondre à la demande d'option pour l'une des modalités de contrôle, ou retarde excessivement son choix,
- le choix exprimé par le contribuable ne permet pas, pour des raisons techniques ou pratiques, de mettre en œuvre la vérification des données ou des traitements (cas notamment de systèmes situés à l'étranger sans possibilité de travail sur le matériel du contribuable, ou communication de copies des informations),
- les données ne sont pas disponibles pour la réalisation du contrôle,
- les données sont disponibles, mais le contrôle n'a pu être mené à son terme du fait de circonstances imputables au comportement du contribuable, à l'organisation de l'entreprise ou à un tiers prestataire notamment,
- les traitements réalisés à partir des données disponibles dans l'entreprise ne répondent pas aux demandes de l'administration,
- les traitements ne sont pas réalisés dans un délai raisonnable.

3) Sanction

Dans l'hypothèse d'une évaluation d'office des bases d'imposition, pour tout ou partie des résultats, les sanctions spécifiques prévues aux articles 1730 et 1755 du CGI s'appliquent (c'est-à-dire, majoration de 150 % des droits supplémentaires mis à la charge du contribuable, taxation d'office et refus de consultation des différentes commissions fiscales).

C. Rappel des textes de référence

- Art. 103 de la loi de finance pour 1990 – Contrôle des comptabilités informatisées.
- Loi du 10 mai 1994 – Programmes développés par des prestataires.
- Arrêté du 13 septembre 1991, pris pour l'application de l'article L. 47 A du livre des procédures fiscales fixant les normes de copies de fichiers produites sur support informatique modifié par l'arrêté du 31 décembre 1996.
- Instruction du 14 octobre 1991 – Contrôle des comptabilités informatisées (BOI 13 L-6-91).
- Instruction du 24 décembre 1996 – Contrôle des comptabilités informatisées (BOI 13 L-9-96).

2.2. Protection des informations nominatives

2.2.1. Les données concernées

La loi du 6 janvier 1978 définit les informations nominatives comme « les informations qui permettent, sous quelque forme que ce soit, directement ou non, l'identification des personnes physiques auxquelles elles s'appliquent, que le traitement soit effectué par une personne physique ou une personne morale ».

Sont concernées les informations permettant d'identifier directement ou indirectement une personne : coordonnées administratives (adresse, numéro de téléphone, numéro de sécurité sociale, etc.), données concernant l'état civil (nom, prénom, sexe, date et lieu de naissance) ou l'aspect physique (image, voix, empreintes digitales ou génétiques).

Certaines de ces informations peuvent, sous réserve de satisfaire aux obligations prescrites par la loi (et décrites ci-dessous) faire l'objet d'un traitement automatisé :

- les informations relatives aux opinions politiques, philosophiques ou religieuses, les appartenances syndicales ou les mœurs des personnes, ne peuvent faire l'objet de traitements automatisés, sans l'accord exprès de l'intéressé,
- les informations comme le numéro de sécurité sociale, les condamnations pénales, la race ou encore la santé, ne pourront être traitées par certaines instances, qu'après autorisation par décret en Conseil d'État pris après avis de la CNIL, en raison de leur caractère hautement « sensible ».

Le traitement automatisé est défini par la loi comme « tout ensemble d'opérations réalisées par les moyens automatiques, relatif à la collecte, l'enregistrement, l'élaboration, la modification, la conservation et la destruction d'informations nominatives ainsi que tout ensemble d'opérations de même nature se rapportant à l'exploitation de fichiers ou bases de données et notamment les interconnexions ou rapprochements, consultations ou communications d'informations nominatives ».

Sont concernés tous les systèmes automatisés dès lors qu'ils portent sur des données nominatives. On peut notamment citer :

- les fichiers informatiques et logiciels en permettant l'exploitation,
- les cartes à puce,
- les autocommutateurs téléphoniques,
- les systèmes d'accès physique à des locaux (contrôles d'accès par badges),
- les systèmes d'accès logique à un réseau (identification des personnes par un code d'accès).

La CNIL est une autorité administrative indépendante qui a pour mission essentielle de protéger la vie privée et les libertés individuelles ou publiques. Elle est chargée de veiller au respect de la loi "Informatique et libertés" qui lui confie six missions principales :

- recenser les fichiers,
- contrôler,
- réglementer,
- garantir le droit d'accès et de rectification,
- instruire les plaintes,
- informer.

Aucun traitement automatisé d'informations nominatives ne peut être mis en œuvre sans que des formalités préalables n'aient été accomplies auprès de la CNIL.

Une entreprise devra déclarer à la CNIL tous les fichiers faisant l'objet d'un traitement nominatif. Parmi les exemples les plus courants, on trouve :

- les fichiers clients,
- les fichiers fournisseurs,
- les fichiers de paye des employés,
- les fichiers de prospect commercial…

2.2.2. Le droit des personnes par rapport aux données collectées

Les droits des personnes dont les données nominatives sont enregistrées dans un traitement automatisé sont les suivants :

- droit d'être informé du traitement des données :
  - l'intéressé doit être informé du caractère obligatoire ou facultatif de la collecte, des conséquences d'un défaut de collecte, des destinataires des informations, de l'existence d'un droit d'accès et de rectification aux informations le concernant. Chaque infraction est passible d'une contravention de police de 5e classe,
  - l'information des personnes peut en principe être effectuée par tous moyens, sauf lorsque les renseignements sont collectés sous forme de questionnaire. Dans ce cas, la loi précise que l'information prévue doit figurer sur ces questionnaires (loi du 6 janvier 1978, art. 27, al. 2),
- droit d'accéder et de rectifier les informations qui y sont contenues :
  - dès lors qu'elle justifie de son identité, toute personne fichée bénéficie d'un droit d'accès et de rectification sur des informations nominatives la concernant (art. 34). Le fait de s'opposer au droit d'accès ainsi qu'à la communication des informations est sanctionné par une contravention de police de 5e classe,
- droit de s'opposer au traitement des données :
  - les modalités de mise en œuvre de ce droit ne sont pas précisées par la loi. Il revient donc au juge, en cas de litige, d'apprécier la « légitimité » des raisons invoquées par celui qui s'oppose au traitement,
  - le fait de collecter des données malgré l'opposition de la personne concernée est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (art. 226-18 du Code pénal).

2.2.3. Les obligations et les formalités à accomplir

Le responsable est le décideur du traitement, c'est-à-dire le détenteur direct ou indirect (signature par délégation) des pouvoirs permettant d'engager l'entreprise ou l'organisme. Un organisme qui crée un traitement, mais en sous-traite l'exploitation, est responsable du traitement.

En plus du respect des droits des personnes énoncés ci-dessus, la loi prévoit une obligation :

- de déclaration des traitements :
  - la déclaration doit être établie par le responsable du fichier, c'est-à-dire celui qui a le pouvoir de décider de la création du traitement (formulaire type complété par des annexes, disponible auprès de la CNIL),
  - le non respect de cette formalité préalable est pénalement sanctionné de trois ans d'emprisonnement et de 45 000 euros d'amende (art. 226-16 du Code pénal),
- de ne pas utiliser le traitement à d'autres fins que celles déclarées :
  - la CNIL peut évaluer si les données enregistrées sont « adéquates, pertinentes et non excessives », en fonction de la finalité déclarée par le responsable du traitement. Tout

changement de finalité d'un traitement déclaré doit être signalé à la CNIL (déclaration de modification),

- le fait de détourner un traitement d'informations nominatives de la finalité qui lui a été attribuée lors de sa création est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende (art. 226-21 du Code pénal),

- de sécurité :
  - le responsable d'un traitement d'informations nominatives s'engage, vis-à-vis des personnes concernées, à prendre toutes les précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles soient déformées, endommagées ou communiquées à des tiers non autorisés (art. 29 de la loi Informatique et Liberté du 6 janvier 1978). C'est pourquoi, la déclaration doit expressément préciser les dispositions prises pour assurer la sécurité des traitements et des informations,
  - le manquement à la sécurité est également sanctionné car « le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende » (art. 226-17 du Code pénal),
  - de plus, le fait de divulguer des informations nominatives ayant pour effet de porter atteinte à l'intéressé ou à sa vie privée est puni d'un an d'emprisonnement et de 15 000 euros d'amende lorsque la divulgation est intentionnelle et de 7 500 euros d'amende lorsqu'elle est commise par imprudence ou négligence (art. 226-22 du Code pénal).

2.3. Protection des logiciels

La protection des logiciels est réglementée par le Code de la propriété intellectuelle. Les logiciels mis à la disposition du public par la diffusion d'un support matériel sont soumis à l'obligation de dépôt légal à la Bibliothèque Nationale. Le dépôt est obligatoire et gratuit. Il est sanctionné par des peines d'amende allant de 1 500 à 75 000 euros.

L'Agence pour la Protection des Programmes (APP) a pour objet l'inscription et la protection des œuvres numériques.
L'objet de l'APP est décrit dans l'Article 1 du règlement général APP-IDDN : « L'Agence pour la Protection des Programmes (APP), organisation européenne des auteurs de logiciels et concepteurs en technologie de l'information, association régie par la loi française du 1er juillet 1901, a pour objet de défendre les personnes physiques ou morales, auteurs, éditeurs ou producteurs de programmes informatiques, de jeux vidéo, de progiciels, d'œuvres numériques, d'études et de documents associés ».

Les auteurs de logiciels peuvent déposer auprès de cette association les codes sources, notamment pour des raisons probatoires. Dans ce cadre, l'APP s'occupe de faciliter les actions amiables ou judiciaires tendant à la réparation des préjudices subis par le titulaire des droits du fait de contrefaçons ou d'imitations frauduleuses ou illicites.

Organisme de défense professionnelle, l'APP en vertu de l'article L. 331-1, alinéa 2 du Code de la propriété intellectuelle, a qualité pour ester en justice pour défendre les intérêts des créateurs. L'APP attribue à chaque œuvre inscrite à son répertoire (dépôt ou référencement) un identifiant international IDDN (Inter Deposit Digital Number).

Au niveau international, la Business Software Alliance (BSA) est une organisation qui représente les principaux développeurs de logiciels et du commerce électronique dans 65 pays. Elle a été fondée en 1988 et possède des bureaux aux Etats-Unis, en Europe et en Asie. Son action consiste à sensibiliser les gouvernements et les consommateurs à la lutte contre la fraude relative aux logiciels et le vol sur Internet.

Cette association met à disposition (par téléchargement) des consommateurs et des entreprises un logiciel d'audit, GASP, permettant d'identifier les copies illicites figurant sur un ou plusieurs ordinateurs.

Le tableau suivant présente une synthèse des infractions par type de logiciels.

2.3.1. Logiciels téléchargeables :

	Typologie		**Infractions**	**Etendue de la protection**
Téléchargement possible	**Logiciels libres (open source)**	L'auteur fournit gratuitement le logiciel avec son code source.	En général le contrat de licence exclut l'exploitation commerciale du logiciel libre.	Les droits sont régis par les termes du contrat de licence. Le droit de paternité, au même titre que les autres droits moraux, a une durée illimitée.

	Logiciels gratuits (freeware)	L'auteur a donné son accord pour la reproduction et l'exploitation du logiciel sans contrepartie.	Utilisation, copie et diffusion gratuites autorisées. Mais interdiction de modification sans le consentement de l'auteur.	Droits d'auteur limités au contenu.
	Logiciels à l'essai (shareware)	L'auteur a donné son accord avec des contreparties (conditions d'utilisation et/ou paiement demandé).	L'utilisation du logiciel sans respecter les conditions du contrat de licence ou sans payer le montant de la redevance constitue un acte de contrefaçon. L'auteur doit avoir exprimé les conditions dans lesquelles il consent à l'utilisateur un droit de reproduction et d'utilisation. A défaut, le téléchargement est un acte de reproduction et l'utilisation du logiciel sans droit constituerait nécessairement un acte de contrefaçon.	Les droits sont régis par les termes du contrat de licence.
	Logiciels du domaine public	Les auteurs ont renoncé à leur droit de paternité sur l'œuvre.	Aucune, libre disposition.	Pas de droits de paternité sur ces logiciels.

2.3.2. Logiciels non téléchargeables :

		Droits de l'utilisateur du logiciel	**Droits de l'auteur du logiciel**		**Infractions**		**Sanctions**
Téléchargement prohibé	**Logiciels commerciaux**	▪ Droit d'utilisation ▪ Droit de décompilation du logiciel sous certaines conditions ▪ Droit à une seule copie de sauvegarde ▪ Droit de reproduction et de traduction du code pour les besoins de l'interopérabilité, dans les conditions stipulées par le Code de la propriété intellectuelle	Droits d'auteur accordés pour 70 ans	Droits moraux : ▪ Droit au nom ▪ Droit au respect de l'œuvre ▪ Droit d'autoriser ou non la divulgation de son oeuvre Droits patrimoniaux : ▪ Droit d'exploitation (d'utilisation et d'usage) ▪ Droit de représentation ▪ Droit de reproduction ▪ Droit de traduction, d'arrangement, d'adaptation ▪ Droit de mise sur le marché à titre gratuit ou onéreux	Contrefaçon et dommages et intérêts si l'auteur a subi un préjudice lié à l'utilisation sans licence.	*Loi du 10 mai 1994 Loi du 5 février 1994*	Responsabilité civile et pénale du dirigeant d'entreprise personne physique en plus de celle de la personne morale.

3. THEME 3 : LES PARTICULARITES EN ENVIRONNEMENT PROGICIEL DE GESTION INTEGRE (PGI)

3.1. Description générale

L'existence d'un progiciel de gestion intégré (PGI) dans une entreprise, en exploitation ou à l'état de projet, peut nécessiter des contrôles spécifiques par le commissaire aux comptes. Il est en effet généralement plus difficile d'appréhender des progiciels que des applications spécifiques, en raison de l'existence de paramètres et d'habilitations.

Le système d'information apparaît fermé en première approche, rendant difficiles les travaux de contrôle interne. La connaissance du système par les salariés de l'entreprise est parfois limitée car ils n'ont pas toujours été impliqués dans la mise en place du progiciel ou bien ont été insuffisamment formés. Aussi, ils ne comprennent pas nécessairement toutes les conséquences et les incidences multiples que peuvent avoir leurs actions sur le système d'information, ainsi que sur les données comptables et financières.

3.1.1. Caractéristiques du progiciel de gestion intégré (PGI)

Il est utile de recueillir des informations concernant les caractéristiques du progiciel de gestion intégré utilisé par l'entreprise, tant l'offre des éditeurs est hétérogène. Le système a pu être conçu initialement de manière globale et intégrée ou avoir été développé autour de fonctionnalités spécifiques, comme par exemple la comptabilité.

On distingue généralement trois grandes catégories de systèmes :

- les PGI destinés aux grandes entreprises, dont les fonctionnalités sont très développées en matière de gestion des devises, d'adaptation à l'organisation de l'entreprise et couvrant l'ensemble des activités,
- les PGI destinés aux entreprises de taille moyenne, dont les fonctionnalités peuvent se limiter au périmètre comptable et aux domaines directement liés, comme les achats et dans lequel il est possible de gérer plusieurs entités juridiques,
- les PGI destinés aux petites entreprises, dont les fonctionnalités réduites ne permettent généralement pas une prise en compte des particularités de l'entreprise.

3.1.2. Stratégie informatique de l'entreprise

La stratégie informatique de l'entreprise et les modalités de mise en place du PGI sont des informations importantes pour apprécier les risques informatiques.

Deux stratégies opposées peuvent être adoptées par l'entreprise quant à la mise en place du PGI :

- refonte complète des processus de l'entreprise pour s'adapter à la structure et aux fonctionnalités du PGI,
- adaptation du PGI à l'organisation et aux particularités de l'entreprise.

Un élément important de la stratégie de mise en place concerne le choix fait par l'entreprise de faire appel ou non à une société de services externe et ses conséquences sur :

- les modalités de paramétrage du progiciel,
- le niveau de maîtrise du progiciel par l'entreprise et son niveau de dépendance vis-à-vis du tiers.

3.1.3. Contexte d'intervention

Dans la mission d'audit, lors de la phase « Orientation et planification de la mission », il convient d'examiner les caractéristiques du projet informatique, pour identifier dans le plan de mission, les contrôles à effectuer dans la phase « Evaluation des risques ».

3.1.4. Cartographie

La cartographie est un outil permettant d'avoir une vue générale du système d'information de l'entreprise, afin d'en comprendre le fonctionnement et d'organiser les contrôles à effectuer dans le cadre de la mission d'audit.

Il est pertinent d'identifier le périmètre des fonctionnalités installées et paramétrées par l'entreprise :

- une première approche consiste à prendre connaissance de la documentation fournie par l'éditeur et à identifier avec l'entreprise les modules qui ont été paramétrés. Certains progiciels peuvent offrir ces informations au niveau du module d'administration,
- une seconde approche consiste à rechercher le contrat de licence, qui généralement détaille les modules qui ont été acquis et peut également donner des informations sur les profils utilisateurs (paramétrage, utilisation, consultation). Certains PGI sont installés en standard avec tous les modules, même si l'entreprise n'en utilise qu'une partie.

Les informations recueillies permettent d'identifier les éléments sensibles qui pourront faire l'objet d'un contrôle détaillé, par exemple les points d'intégration entre les différents modules (parfois appelés interfaces internes, par opposition aux interfaces externes qui permettent au PGI de communiquer avec d'autres systèmes).

3.2. Evaluation des risques

3.2.1. Les habilitations

La gestion des droits d'accès est un domaine qui doit être étudié systématiquement. Le choix d'un PGI conduit à regrouper au sein d'une même application de nombreuses fonctionnalités, qui auparavant pouvaient être réparties entre plusieurs systèmes. Par exemple, la gestion du cycle achats peut intégrer les fonctionnalités suivantes :

- le référencement fournisseurs,
- la passation des commandes,
- la vérification des bons de livraison,
- le rapprochement factures,
- le paiement.

Le principe de séparation des fonctions est plus facile à respecter par une entreprise utilisant des systèmes différents, en donnant par exemple à une seule personne l'accès à l'application comptable. Dans un progiciel de gestion intégré, toutes les fonctionnalités sont regroupées dans la même application et l'entreprise doit établir la séparation des fonctions à l'aide des habilitations.

La gestion des habilitations, élément essentiel de la sécurité logique, permet généralement de définir des profils utilisateurs types. Il convient de prendre connaissance :

- de la manière dont la gestion des habilitations a été réalisée, car certaines entreprises ont pu par défaut accorder les mêmes droits d'accès à l'ensemble des utilisateurs,
- de la documentation communiquée par l'éditeur.

Il est également nécessaire de vérifier les paramètres généraux de sécurité, leur absence étant considérée comme une faiblesse générale du système d'information :

- gestion des mots de passe (longueur, fréquence de renouvellement…),
- protection du poste de l'utilisateur (blocage en cas de tentatives de connexion, déconnexion automatique passé un certain délai sans utilisation),
- historique des opérations effectuées par les utilisateurs.

3.2.2. Le paramétrage

Une des caractéristiques principales d'un PGI est le paramétrage étendu de ses applications. Le paramétrage permet, dans une certaine mesure, d'adapter le système au fonctionnement et aux particularités de l'entreprise. Si les possibilités de paramétrage peuvent être très développées, les différences, dans les modes de fonctionnement et d'organisation des entreprises d'un même secteur, sont nombreuses. Les entreprises ne se contentent pas généralement du paramétrage « standard » proposé par le PGI et cherchent à l'adapter à leur mode de fonctionnement (modification des programmes, développement de fonctionnalités complémentaires).

Ainsi, avant d'analyser le paramétrage d'un PGI, il est nécessaire de connaître les conditions dans lesquelles il a été installé et a fait l'objet d'éventuelles adaptations :

- une adaptation ou une modification des fonctionnalités de paramétrage par l'entreprise fera l'objet d'une analyse identique à celle qui serait menée en présence d'un logiciel développé en interne : analyse des besoins, des programmes, de la structure des fichiers…,
- une utilisation standard des fonctionnalités de paramétrage par l'entreprise fera l'objet de contrôles simplifiés.

Toute revue de paramétrage devrait débuter par :

- l'analyse de la documentation disponible nécessaire à une bonne compréhension du fonctionnement du PGI,
- l'analyse des domaines sensibles du PGI correspondant aux domaines étudiés dans le cadre de la mission d'audit. En effet, la complexité de la majorité des PGI rend absolument impossible la réalisation d'une revue « complète » du paramétrage.

La revue du paramétrage consiste à étudier les règles de gestion « métiers » et les règles de gestion financières.

A. Règles de gestion « métiers »

Les règles de gestion « métiers » consistent dans le paramétrage des modules concernés par les processus de l'entreprise (achats, ventes, stocks…). Les choix réalisés par l'entreprise ainsi que l'existence d'anomalies de paramétrage ayant une incidence directe sur la génération des comptes, il est par conséquent nécessaire de ne pas limiter les contrôles aux applications comptables seules.

B. Règles de gestion financière

L'analyse des règles de gestion financière dans un PGI concerne non seulement les paramètres standards communs à toute application comptable (plan de compte, taux de TVA, fréquence de facturation…), mais également les points d'intégration, appelés interfaces internes, qui permettent le transfert de données entre les différents modules.
S'il n'existe pas de règles générales pour les interfaces internes, il est fréquent de rencontrer les situations suivantes :

- les paramètres permettant l'intégration entre deux modules sont généralement définis dans le module le plus en « amont » (exemple : les paramètres de la comptabilité des achats sont gérés dans le module « gestion des commandes »). Le paramétrage revient souvent à la définition d'un type ou d'une catégorie (par exemple une catégorie d'achat, un type de commande). Il sera donc recherché la manière dont ces paramètres sont définis et dont le lien est fait avec le module de comptabilité,
- les liens entre les modules peuvent être réalisés :
  - soit par une table de correspondance (par exemple, entre un type d'achat et un compte de la classe 6), permettant un passage automatique des données entre deux modules,
  - soit par un paramétrage au niveau de la transaction, c'est-à-dire que la donnée, par exemple la commande, contient les différents paramètres (type d'achat, numéro de compte). Les données sont alors directement accessibles par les différents modules.

3.2.3. Référentiels

Il s'agit des bases de données utilisées dans les programmes. En fonction des progiciels, il peut exister un ou plusieurs référentiels. On rencontre généralement les situations suivantes :

- le référentiel de l'organisation de l'entreprise est commun à l'ensemble des modules pour rendre possible leur intégration,
- concernant les tiers, il existe différents cas, à savoir :
  - les référentiels sont spécialisés par module,
  - un référentiel général regroupe l'ensemble des tiers (clients, fournisseurs voire salariés).

Quel que soit le PGI, l'analyse du référentiel consiste à rechercher l'utilisation qui en est faite par les différents modules. En effet, si un référentiel peut être partagé entre plusieurs modules, il n'est généralement pas utilisé de la même manière. Le référentiel « clients » est par exemple généralement géré dans le module de gestion commerciale, même si certaines informations peuvent être utilisées par d'autres modules (dont la comptabilité auxiliaire client). Certains PGI complexes prévoient un partage des référentiels entre différents modules en donnant à chaque module la possibilité de gérer des données propres, celles-ci étant liées aux données centrales du référentiel.

Cette analyse doit être rapprochée de l'étude des habilitations pour connaître les droits d'accès donnés aux utilisateurs sur les référentiels.

3.2.4. Interfaces externes au PGI

Quels que soient les avantages d'un PGI et la volonté de l'entreprise de mettre en place un système intégré, le système d'information est souvent constitué de plusieurs applications hétérogènes. Les contrôles porteront sur chacune des applications, mais également sur les interfaces permettant le transfert des données.

A. Description

Les interfaces développées autour d'un PGI doivent être décrites en prenant soin d'identifier :
- leur type (entrante/sortante),
- leur degré d'automatisation (intervention ou non de l'utilisateur),
- les modules concernés.

B. Opérations de déclenchement

Les interventions de l'utilisateur peuvent être extrêmement variées :
- intégration/export d'un fichier avec description du format d'entrée ou de sortie (il s'agit dans ce cas davantage d'une structure de fichier d'échange, que d'une interface au sens strict du terme),
- déclenchement manuel d'un traitement automatique,
- simple vérification du traitement des exceptions ou des rejets de l'interface.

Il est nécessaire de rechercher l'existence d'un module spécifique pour la gestion des interfaces. C'est généralement le cas pour les interfaces sortantes via des fonctionnalités d'export de données. Concernant l'import de données, il convient de rechercher les fonctionnalités permettant aux utilisateurs de suivre le bon fonctionnement des interfaces, comme par exemple :
- le suivi des traitements (statut, respect de la fréquence prévue…),
- l'identification des éventuels rejets,
- la possibilité de connaître la cause des rejets et de retraiter les données concernées.

C. Interfaces normées / non normées

Avant de contrôler les interfaces, il est nécessaire d'identifier le type d'interface offert par le PGI, en particulier pour les interfaces entrantes.

On peut classer les interfaces selon quatre catégories principales :
- les interfaces utilisant un langage ou un module spécifiquement proposé par l'éditeur. Ce module utilise généralement les fonctions du PGI, les données intégrées par l'interface subissant les mêmes contrôles que les données saisies manuellement par l'utilisateur,
- les interfaces utilisant le langage ou un module proposé par le système de gestion de la base de données (SGBD). Dans ce cas, si les données subissent bien les contrôles propres au SGBD (contrôle de cohérence des données), elles ne seront pas soumises aux contrôles « fonctionnels des applications ». Ces contrôles plus riches peuvent concerner par exemple des vérifications de calculs (type cohérence montant hors taxe, montant TVA, montant TTC),
- les interfaces spécifiques utilisant un langage normalisé comme dans le cas des échanges EDI. Il est possible d'utiliser ce type d'échange entre deux systèmes internes à l'entreprise,

- les autres interfaces utilisant différents moyens non prévus par l'éditeur du PGI (modification des programmes, écritures directes dans les tables de la base de données…).

Le contrôle des interfaces doit passer par la compréhension du type d'interface concernée, afin d'identifier les travaux de contrôle interne pertinents à mener et d'apprécier les risques associés. On considère en général qu'une interface standard qui se situe au niveau de l'applicatif présente peu de risques, car les données intégrées en provenance d'une application externe subissent alors les mêmes contrôles que les données saisies directement dans l'application.

D. Méthodes de contrôle

Si les méthodes de contrôle varient selon le type d'interface, l'objectif reste le même dans tous les cas. Il s'agit de vérifier le fonctionnement des contrôles mis en place par l'entreprise (vérification du traitement de l'interface selon la fréquence prévue, suivi des contrôles réalisés sur les données, des rejets et de leur traitement…).

Dans le cas où l'entreprise n'utilise pas les possibilités d'interface offertes ou s'il n'existe pas d'interface, l'analyse portera sur les points suivants :
- étude du fonctionnement général (traitement, circulation des fichiers),
- analyse des contrôles programmés,
- sondage sur certains fichiers avec comparaison des fichiers en sortie de l'application amont et en entrée de l'application aval.

3.2.5. Etats

L'existence d'un PGI dans une entreprise modifie souvent les méthodes de travail des utilisateurs, lesquels peuvent utiliser directement des fonctionnalités de recherche ou de tri, au détriment des états comptables.

A. Etats standards

1) Etats comptables

- balance générale,
- balances auxiliaires (clients, fournisseurs),
- registre des immobilisations,
- états préparatoires d'inventaires physiques…

2) Etats de gestion

Dans cette catégorie, sont généralement proposés des états qui peuvent être utilisés comme tableau de bord. Cependant, il est important de noter que plus un PGI offre de possibilités de paramétrage, plus il est difficile pour un éditeur de proposer des états standards de gestion. Dans ce cas, la préparation et le développement de ces états doivent être réalisés par l'entreprise au cours de l'installation du PGI.

Pour cela, deux solutions existent :

- le progiciel comprend un module standard ou un programme complémentaire dédié à la préparation d'états de gestion,
- le progiciel ne propose pas une telle solution et il est alors nécessaire de faire appel à un progiciel spécialisé qui accédera à la base de données pour utiliser les données de l'application et réaliser les traitements, regroupements et présentations nécessaires à la réalisation des états de gestion.

3) Etats financiers

Ces états sont généralement proposés par l'ensemble des PGI. Ils comprennent au minimum le bilan et le compte de résultat. Cependant, selon le PGI et la méthode utilisée par l'éditeur, ces états devront être modifiés pour tenir compte de certains paramétrages, par exemple lorsque l'entreprise a modifié le plan de compte standard proposé par l'éditeur.

B. Etats spécifiques

Il convient de distinguer parmi les situations suivantes :

- présence d'un module de génération d'états spécifiques (qui est généralement proposé dans l'ensemble des PGI, le nombre d'états standards proposés par défaut étant en général réduit),
- présence d'un logiciel complémentaire externe, éventuellement proposé par l'éditeur, dédié à la réalisation des états de gestion.

Ensuite, il s'agit d'identifier les états spécifiques utiles à la mission d'audit et de vérifier leur cohérence avec les données de l'application, ainsi que l'exactitude des calculs réalisés par le générateur d'états. Si l'entreprise utilise un grand nombre d'états spécifiques, il est conseillé d'effectuer un examen détaillé de ces états, des erreurs commises dans la conception étant souvent à l'origine d'erreurs dans l'enregistrement des opérations.

3.2.6. Piste d'audit

A. Présentation

Dans un PGI, la piste d'audit recouvre une importance particulière car elle permet de retrouver une pièce justificative. En effet, dans une application comptable classique, lors de l'enregistrement d'une écriture, un utilisateur saisit également une référence permettant de retrouver la pièce justifiant l'écriture comptable (cette pièce pouvant être par exemple une facture).

Dans un PGI, les écritures peuvent être enregistrées dans le module comptabilité sans faire l'objet d'une saisie directe. Le commissaire aux comptes, qui souhaitera à partir d'une écriture consulter une pièce justificative, ne sera pas toujours en mesure de retrouver directement la référence de cette pièce.

En revanche, la majorité des PGI peut être paramétrée afin de pouvoir suivre une opération entre les différents modules qui le composent. Il doit être possible de suivre une piste d'audit, soit par utilisation des références, soit directement par des fonctionnalités dites « drill-down ».

B. Piste d'audit dynamique

La majorité des éditeurs propose dans leur offre des fonctionnalités de piste d'audit dynamique qui permettent d'identifier les opérations qui sont à la source d'une écriture comptable. Par exemple, une écriture d'achat passée dans la comptabilité fournisseurs peut trouver son origine dans le module achats. Une fonctionnalité de piste d'audit dynamique doit permettre, à partir de l'écriture comptable, de revenir au document de base (une facture par exemple), voire à toutes les opérations liées à ce document et présentes dans le système (exemples : un bon de livraison, un bon de commande, une demande d'achat).
Si ces fonctionnalités présentent un intérêt évident pour les utilisateurs, elles peuvent également être mises à profit par le commissaire aux comptes afin d'analyser un compte. Généralement, un PGI propose une fonctionnalité permettant de partir du solde du compte pour retrouver les écritures et remonter aux opérations d'origine effectuées dans les modules en amont.

3.2.7. Les techniques d'audit assistées par ordinateur

Comme indiqué au chapitre « Méthodologie », les techniques d'audit assistées par ordinateur sont utilisées essentiellement dans la phase « Obtention d'éléments probants ». Dans le cadre d'un PGI, elles peuvent satisfaire les objectifs suivants :

- vérifier, par l'utilisation d'un jeu de tests, le correct paramétrage et l'exactitude d'un calcul effectué par le PGI,
- vérifier un calcul avec des données réelles, par exemple une dotation aux amortissements.

Les principes de l'analyse de données en environnement PGI ne diffèrent pas fondamentalement des contrôles effectués dans un autre environnement informatisé (qu'il s'agisse d'une application spécifique ou d'un progiciel comptable).

En revanche, la nature du PGI peut avoir un impact important sur l'analyse de données. Plus le PGI est complexe et moins la structure de la base de données est accessible aux contrôles. Les contrôles suivants peuvent alors être effectués :

- utilisation des fichiers d'interfaces : ils sont généralement faciles à obtenir et présentent un format défini et connu des utilisateurs. Ils ne permettent pas d'effectuer des contrôles sur les données internes à un ou plusieurs modules,
- utilisation des exports spécifiques demandés à l'entreprise : ils peuvent nécessiter l'intervention d'un prestataire, l'entreprise ne disposant pas toujours des compétences internes nécessaires.

Dans de nombreux environnements, il est possible d'utiliser un module d'export de données proposé par l'éditeur (soit dans le PGI lui-même, soit grâce à un module complémentaire). Cette opération nécessite la connaissance de la structure des données. La documentation utilisateur est généralement insuffisante sur ce point ; il est alors indispensable d'étudier la documentation technique ou une documentation spécialisée mise à disposition par l'éditeur.

En règle générale, l'analyse de données dans un environnement PGI devrait être limitée au maximum car elle peut s'avérer complexe et longue à mettre en œuvre. Il existe généralement d'autres moyens d'atteindre les résultats attendus, comme la revue du paramétrage et des habilitations.

4. THEME 4 : LES PARTICULARITES EN ENVIRONNEMENT INTERNET

Ce dossier thématique présente les principales particularités, juridiques et techniques, d'un environnement Internet.

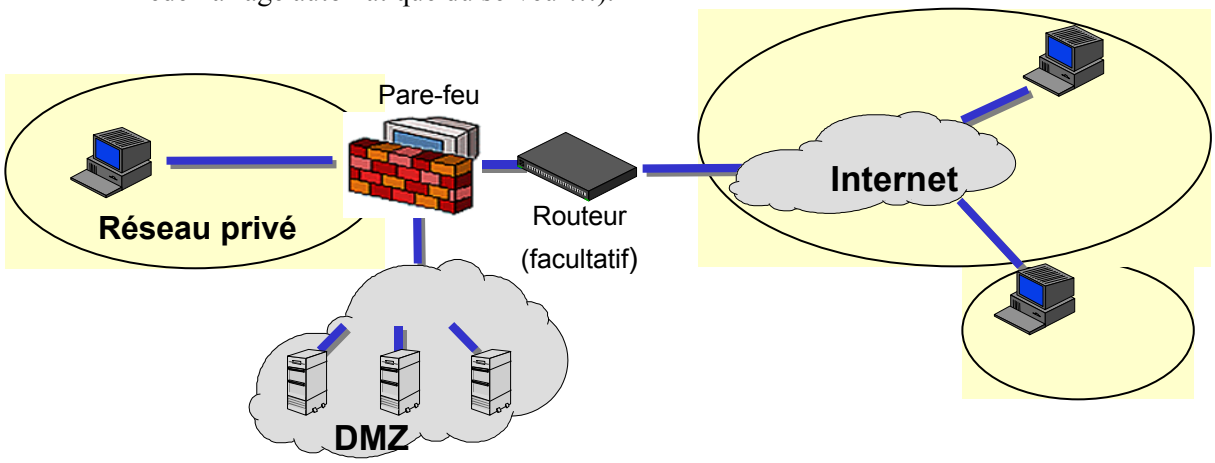
L'objet n'est donc pas ici de procéder à un audit qualité d'un site Internet, comme c'est le cas lors d'une intervention WebTrust, qui s'attache à vérifier que les obligations réglementaires et qu'un ensemble de critères de qualité sont respectés. Ainsi, si les référentiels WebTrust peuvent être utilisés pour prendre en compte les risques liés à Internet dans la mission d'audit, les contrôles à effectuer dans la mission légale sont plus limités.

Une entreprise utilise Internet notamment pour les opérations suivantes :

- simples publications d'informations sur un site Internet,
- échanges d'informations, communications entre l'entreprise et d'autres acteurs (particuliers ou entreprises), via une messagerie électronique ou un site Internet, avec interventions manuelles (forum, discussion en ligne, messagerie) ou automatiques (moteur de recherche),
- transactions, par exemple l'achat et la vente en ligne (commerce électronique), la gestion de comptes bancaires, les déclarations administratives…,
- intégration de services (achat, logistique, production…) entre fournisseurs et clients ; on parle alors d'activités e-business, délivrées la plupart du temps au travers d'un extranet.

Les principales caractéristiques d'un environnement Internet, par rapport à un environnement en local (réseau d'entreprise) sont les suivantes :

- une ouverture du réseau de l'entreprise sur l'extérieur, généralement facteur de risques supplémentaires,
- un environnement technique spécifique :
  - un ou plusieurs routeurs permettant l'accès à Internet,
  - un ou plusieurs serveurs pour la publication de pages html, pour la messagerie, les applications, les bases de données. Il est fréquent de rencontrer dans les entreprises la configuration suivante : un serveur de messagerie, un serveur d'applications et un serveur pour la base de données,
  - un ou plusieurs pare-feu (ou firewall), matériel ou logiciel réalisant des fonctions de filtrage au niveau des couches réseau et applicatif,
  - un serveur de surveillance et de contrôle à distance permettant de vérifier l'état des serveurs par des requêtes (de type http, smtp, ftp, https, et pop). En fonction des contrôles, différentes actions peuvent être entreprises (déclenchement d'une alarme, redémarrage automatique du serveur…).

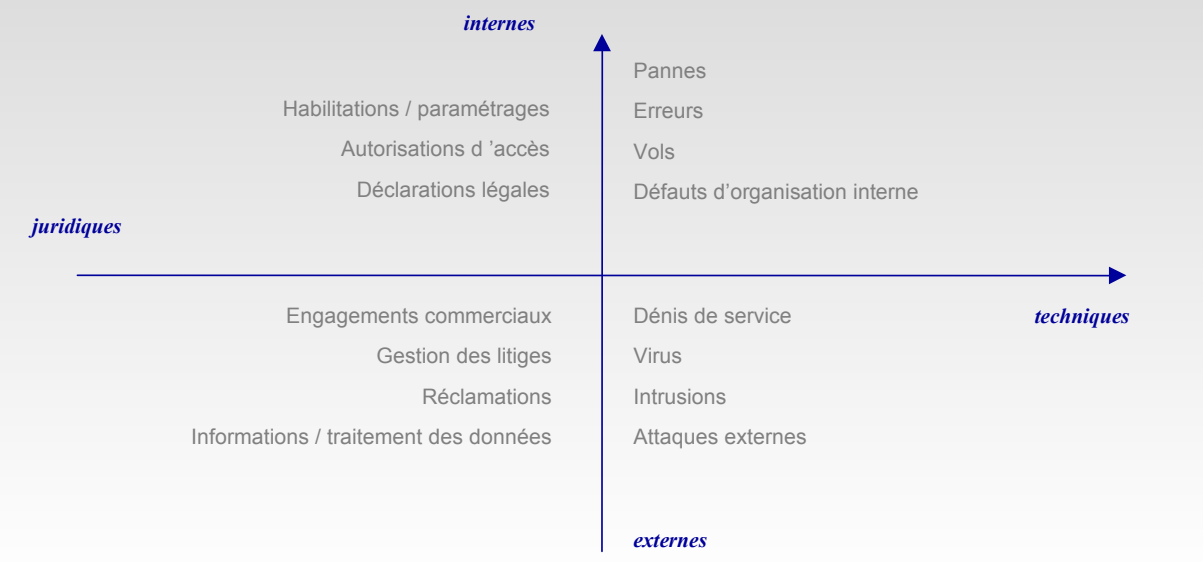


On peut distinguer trois niveaux de complexité dans un environnement Internet :

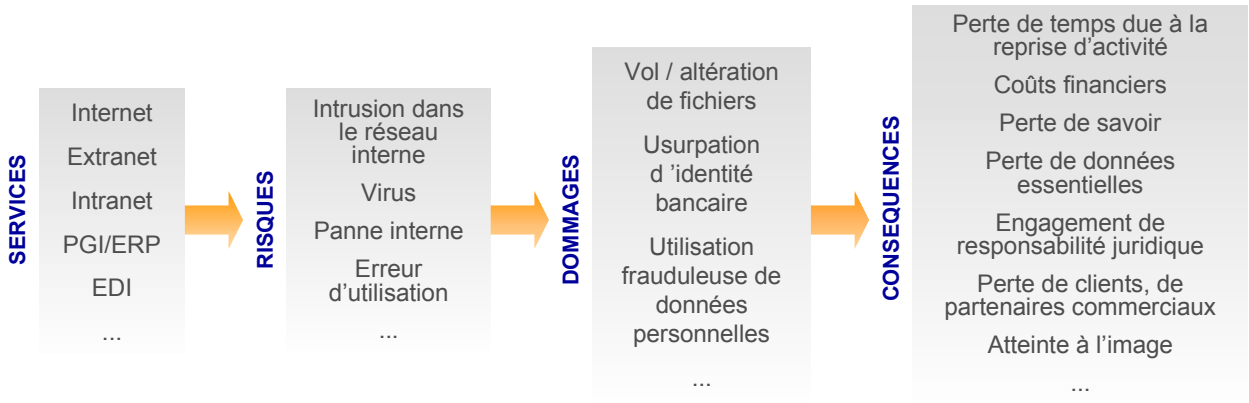
- niveau 1 :
  - utilisation d'une messagerie électronique, soit à partir d'un poste dédié, isolé du réseau de l'entreprise pour des raisons de sécurité ou à partir de l'ensemble des postes,
  - publication d'informations sur un site Internet,
- niveau 2 :
  - ventes en ligne,
  - collecte de données clients (formulaires en ligne…),
  - intranet,
- niveau 3 :
  - extranet,
  - PGI interfacé avec des applications e-business.

4.1. Risques liés à Internet

Le type et le niveau de risque sont fonction des caractéristiques de l'environnement Internet de l'entreprise. Les risques liés à Internet peuvent être synthétisés ainsi :



Le schéma ci-dessous illustre l'enchaînement des risques, des dommages et de leurs conséquences, liés à l'existence de services Internet.



Les principaux risques juridiques, spécifiques ou renforcés par l'Internet, sont les suivants :
- protection des données personnelles,
- pratiques commerciales,
- risques immatériels et responsabilité civile professionnelle,
- fiscalité du commerce électronique,
- publication sur Internet d'œuvres protégées.

Les principaux risques techniques, spécifiques ou renforcés par l'Internet, sont les suivants :
- disponibilité,
- sécurité des transactions,
- intrusions,
- infections virales.

4.1.1. Risques juridiques liés à Internet

Les informations présentées ne visent pas l'exhaustivité, l'objectif étant de présenter les principales problématiques juridiques, souvent complexes et en constante évolution, liées à une activité Internet.

A. Protection des données personnelles

La loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique à la circulation d'informations sur Internet dès lors qu'elles sont nominatives.

Un site Internet, qui par exemple met en ligne des formulaires visant à collecter les données des internautes, doit satisfaire les obligations légales suivantes :
- la nature des données collectées doit être autorisée par la loi,
- les traitements effectués sur les données collectées doivent être déclarés à la CNIL et tout changement dans la nature des traitements doit lui être communiqué,
- l'entité responsable de la collecte et du traitement des données doit mettre en œuvre les mesures de sécurité nécessaires pour garantir la confidentialité,
- l'internaute doit être clairement informé de la collecte et du traitement des données effectués : la CNIL considère que les mentions prescrites par l'article 27 doivent apparaître à l'écran ou être fournies oralement, préalablement à la collecte, lorsque cette dernière est effectuée par voie électronique,
- l'internaute doit pouvoir accéder aux données personnelles collectées le concernant et bénéficier d'un droit de modification de ces données,
- l'internaute doit pouvoir s'opposer à la collecte et au traitement des données le concernant.

Il est à noter que le projet de loi de transposition de la Directive 95/46/CE du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et ses incidences sur le dispositif de la loi Informatique et Liberté du 6 janvier 1978, prévoit notamment :
- le renforcement des pouvoirs de la CNIL (investigation, sanction),
- la redéfinition des données sensibles (impliquant le recueil préalable au traitement du consentement de la personne concernée et qui devrait inclure explicitement les données médicales),
- le renforcement des droits des personnes fichées (droit d'opposition au transfert sans motif légitime, obligation d'information des personnes concernées y compris lorsque la collecte s'effectuera auprès de tiers ...).

Il est donc important que l'entreprise mette en place les procédures suivantes :

- évaluation des risques liés aux traitements informatiques,
- information et sensibilisation auprès des parties concernées,
- dispositif de sécurité et confidentialité du traitement des données, formalisé dans un document de référence,
- définition des responsabilités des personnels participant au respect des mesures de sécurité.

Les obligations des entreprises sont supérieures dans un environnement Internet, que dans un environnement en local, comme le montrent différents avis de la CNIL rendus depuis 1995, par exemple dans l'utilisation des annuaires professionnels.

Enfin, les outils de marketing relationnel (Customer Relationship Management ou Gestion de la Relation Client), permettant la constitution de profils et de segmentation clients, ne peuvent pas être complètement automatisés. La loi prévoit en effet, qu'« aucune décision administrative ou privée impliquant une appréciation sur un comportement humain ne peut avoir pour seul fondement un traitement automatisé d'informations donnant une définition du profil ou de la personnalité de l'intéressé ».

B. Pratiques commerciales

1) Généralités

Le Code de la consommation dans sa quasi totalité régit le commerce électronique.
Le principe de base qui le sous-tend est la protection du consommateur :

- le consommateur ne doit pas être trompé sur la qualité du produit. Le Code de la consommation définit le délit de tromperie relatif à ce principe en son article L. 213-1,
- quant aux informations communiquées au consommateur, le Code de la consommation définit le délit de publicité mensongère, ou de publicité de nature à induire en erreur (art. L. 121-1),
- le Code de la consommation définit des signes de qualité, sous la dénomination « certification de produits et services » (art. L. 115-27) qui s'applique à tous les produits industriels et aux services de même qu'au commerce électronique.

Le principe de la territorialité du droit applicable est une question fondamentale. Le droit français retient que c'est le droit du pays du client qui régit la transaction, en vertu des principes posés par le Code de la consommation lui-même. Cette position est commandée par une philosophie protectrice du consommateur. Au niveau européen, le débat de savoir si le droit du pays du vendeur s'applique est toujours d'actualité.

Néanmoins, les règles protectrices du consommateur sont des règles d'ordre public dont le juge fait application même lorsque le contrat conclu n'est pas soumis à la législation française.

Des textes communautaires non encore transposés sont susceptibles de modifier les règles applicables aux opérations de commerce électronique :

- directive européenne du 8 juin 2000 sur le commerce électronique,
- directive européenne du 23 septembre 2002 concernant la commercialisation à distance de services financiers.

2) Rôle de la DGCCRF en matière de commerce électronique

La forte progression du commerce électronique en France, de 50 % entre avril 2001 et avril 2002, explique que la Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes (DGCCRF) se positionne sur ces sujets malgré le nombre encore relativement faible de vendeurs en ligne.

La structure de la DGCCRF n'était pas initialement adaptée à la surveillance des activités commerciales sur Internet : une structure territoriale, composée de huit laboratoires en France, une direction nationale et une école. Cette organisation s'accordait mal avec une mission de surveillance des réseaux électroniques.

La DGCCRF s'est dotée d'une organisation particulière avec la création de deux structures :

- une structure de réflexion, la MEN, Mission Economique Numérique :
  - la MEN a été créée en 2000 pour une durée de 5 ans. Elle a pour vocation de contribuer à l'adaptation du cadre juridique du commerce électronique et de mener une réflexion sur l'économie numérique (adaptations techniques et financières au sens large),
  - la MEN est subdivisée en neuf groupes dont les sujets de travail sont les problèmes macro-économiques, les technologies de l'information des petites et moyennes entreprises, le droit de la concurrence, le paiement en ligne, la sécurité et les procédures, les aspects internationaux, les sceaux et certifications,
  - à la base de la création du dernier groupe, se trouvent les préoccupations des consommateurs qui redoutent l'immatérialité du commerce électronique. Le besoin étant la confiance, la certification est ressentie de manière pressante et importante,
- une structure d'action, le CSCE, Centre de Surveillance du Commerce Electronique : le CSCE a été lancé le 1er janvier 2001. Il s'appuie sur une équipe d'une dizaine d'agents et un réseau d'enquêteurs spécialisés agissant sur le terrain.

Un site de commerce électronique ne peut se prévaloir de respecter la législation et mettre en avant cette information en tant qu'avantage concurrentiel. En effet, le respect de la légalité va normalement de soi et une telle mention peut laisser sous-entendre que les concurrents ne s'y conforment pas. Toutes les garanties apportées au consommateur doivent dépasser le simple respect de la législation.

En matière de certificats et labels dans le domaine du commerce électronique, la certification privée est libre lorsqu'elle ne peut être confondue avec la certification publique.
Quels sont les éléments concrets susceptibles d'entraîner une confusion entre certification publique et contrôle privé, et comment différencier un contrôle privé d'un contrôle public aux yeux des consommateurs ?
Certains mots font partie du domaine public et ne peuvent être utilisés par les certificateurs privés :

- par exemple, le mot « label » est protégé pour ce qui touche au secteur de l'agro-alimentaire en vertu du Code de la consommation. Il ne peut être employé que pour désigner un signe public de qualité,
- pour les produits et services, les termes « certification », « certifié par » ainsi que toute référence à des organismes publics sont interdits d'utilisation en dehors de missions de contrôle public.

Des termes tels que « contrôle », « vérification », « audit », « attestation » peuvent leur être substitués. De même, la référence à un « organisme certificateur » est proscrite dans le cadre de contrôles diligentés par des sociétés privées. Il est également possible pour éviter toute confusion d'indiquer les caractéristiques contrôlées. L'article L. 115-30 du Code de la consommation prévoit des sanctions pour toute contravention à ces règles.

La surveillance des activités commerciales sur Internet de la DGCCRF en 2001 :
- 3 500 sites de commerce électronique ont été recensés en 2001,
- 988 ont été examinés, représentant un taux de contrôle de 28 %,
- 311 sites comprenant des anomalies ont été détectés,
- au total, 369 anomalies ont été constatées.

Parmi ces anomalies :
- 20 % traduisent le non respect des règles de vente à distance (infractions au Code de la consommation),
- 14 % sont de la publicité mensongère,
- 14 % sont de fausses certifications,
- 7 % concernent la publicité sur les prix,
- 5 % sont relatives à des loteries illicites.

128 mises en demeure ont été émises, 67 procès-verbaux intermédiaires ont été dressés et 17 ont finalement été transmis au Parquet dans le cas d'infractions graves nécessitant une sanction.

Les plaintes des consommateurs reçues par la DGCCRF ont été relativement peu nombreuses à ce jour (5 632 courriels reçus en 2001) :
- 35 % concernaient des demandes d'information,
- 35 % concernaient des réclamations. 31 % de ces dernières concernaient des litiges de droit privé (par exemple une erreur sur la couleur d'un produit, qui ne constitue pas une tromperie, à moins qu'elle ne soit délibérée).

La DGCCRF mène depuis 2002 des actions plus coercitives, de manière à accroître la confiance des consommateurs avec le temps.

C. Risques immatériels et responsabilité civile professionnelle

On distingue deux types de préjudices :
- les préjudices directs subis par l'entreprise (matériel, progiciel…),
- les préjudices indirects causés à des tiers et devant faire l'objet de réparations.

En cas de préjudices, feront l'objet d'une recherche :
- les parties assurées,
- l'objet du contrat, c'est-à-dire ce qui est assuré,
- la durée du contrat (date d'effet et date de fin),
- les clauses d'exclusion.

Internet est un facteur d'amplification des risques, compte tenu de l'importance de la chaîne des responsabilités.

La responsabilité civile professionnelle ne couvre que les activités correspondant à l'objet social de l'entreprise. Une entreprise, dont l'objet social ne concerne pas Internet, peut encourir des risques importants lorsqu'elle développe de manière significative des activités en ligne, sans couverture d'assurance spécifique. Exemple : un hôtel qui développe des réservations par Internet ne sera pas couvert (par sa responsabilité civile professionnelle) des préjudices liés à l'activité en ligne.

Dans les années 1985, les assureurs se sont posés le problème de l'évolution des technologies. Les risques liés à Internet sont-ils assurables ? Internet étant le support de l'immatérialité, le problème revient donc à rendre mesurable l'immatérialité pour la rendre assurable.

Comment l'assureur mesure-t-il l'amplification des risques liés à cette dématérialisation, afin de calculer les primes d'assurance ? :

- dimension technique : en vérifiant que le client dispose d'un niveau de sécurité suffisant en terme d'infrastructure technique,
- dimension juridique / contenu : en vérifiant que les informations véhiculées par Internet ou mises en ligne respectent les obligations réglementaires (respect du Code de la consommation, respect de la propriété intellectuelle sur les contenus…),
- dimension temporelle : en vérifiant l'évolution dans le temps (régulièrement ou en temps réel) des risques techniques et juridiques initialement identifiés.

Pour l'assureur, les vrais risques proviennent surtout de l'activité de l'entreprise et moins du réseau Internet en tant que tel. La question qui se pose aux assureurs est de savoir si l'activité Internet entraîne une augmentation significative de leur responsabilité civile professionnelle, compte tenu du fait qu'un évènement est susceptible d'entraîner des risques en série.
Exemple : L'indisponibilité d'un service d'hébergement. Les capacités financières de l'hébergeur doivent permettre d'assurer les préjudices directs et indirects (soit la perte d'image, de marché… consécutives au même évènement) résultant de cette indisponibilité. Dans cette chaîne de préjudices, le recours subrogatoire peut être exercé par toutes les parties lésées si la preuve de la cause peut être établie.

Les entreprises qui ont recours aux nouvelles technologies changent leur mode opératoire. Une entreprise qui fait de la vente par correspondance maîtrise ses conditions générales de vente ainsi que l'application géographique au moment de l'impression. Dès lors qu'elle commerce sur Internet, les paramètres changent. Le fait que le commerçant sur Internet s'adresse au monde entier entraîne-t-il une aggravation des risques et une modification de sa responsabilité civile professionnelle ?

Pour connaître le caractère assurable ou non de son client, l'assureur va chercher à :

- identifier les principaux risques et les vulnérabilités spécifiques à l'ouverture sur Internet et à l'utilisation des nouvelles technologies,
- auditer la chaîne contractuelle depuis les différents prestataires jusqu'aux contrats clients, et à définir les axes d'amélioration.

Le système d'information est appréhendé comme un ensemble relationnel entre objets stratégiques constitués par les données (fichiers, bases, messages...) et les applications (programmes, procédures...), une distinction supplémentaire étant apportée entre l'utilisateur d'informations (objets clients) et les serveurs d'informations (objets fournisseurs).

L'assureur pourra demander que la solidité du système soit testée régulièrement pour continuer à assurer. Il revient à l'assuré de déclarer à l'assureur ce qu'il estime pouvoir constituer une aggravation des risques. La responsabilité induite est délictuelle ou quasi-délictuelle lorsqu'il s'agit d'un site vitrine ou institutionnel. Elle est contractuelle pour les sites de commerce en ligne.

D. Fiscalité du commerce électronique

1) Le lieu de l'imposition directe

a) Problématique fiscale

En raison du caractère mondial du réseau Internet et de l'immatérialité des sites qui permettent aux entreprises de commercer en ligne, le commerce électronique soulève la question de savoir quel pays est en droit d'imposer la marge afférente à la fourniture de services ou de produits, renvoyant ainsi à la notion d'établissement stable.

La notion d'établissement stable permet à un Etat de taxer les bénéfices d'une entreprise de nationalité étrangère sur les activités qu'elle exerce en direct sur le territoire national, en considérant qu'elle y a installé un établissement stable. L'enjeu pour les entreprises est d'éviter la double imposition.

b) Règles applicables, posées par le Comité des affaires fiscales de l'OCDE

Un site Internet ne peut en lui-même constituer un établissement stable. En général, un accord prévoyant l'hébergement d'un site n'aboutit pas à l'existence d'un établissement stable pour l'entreprise qui exerce des activités commerciales par l'intermédiaire de ce site.

Un fournisseur de services sur l'Internet ne constitue pas, sauf dans des circonstances très exceptionnelles, un agent dépendant d'une autre entreprise de manière à constituer un établissement stable de cette entreprise. Si un local où se trouvent des équipements informatiques, tel qu'un serveur, peut, dans certaines circonstances, constituer un établissement stable, il faut pour cela que les fonctions exercées dans ce local soient importantes et constituent en outre un élément essentiel de l'activité commerciale de l'entreprise.

Ainsi, il n'y aura pas établissement stable si les opérations de commerce électronique réalisées à partir du serveur se limitent à des activités préparatoires ou auxiliaires, telles que de la publicité ou de la fourniture d'informations sur des produits ou services sans possibilité d'achat en ligne.

2) Les revenus imposables

a) Problématique

La classification du revenu joue un rôle important en droit fiscal car elle affecte la façon dont le revenu est attribué et imposé. Les transactions commerciales par voie électronique peuvent être classées comme une vente de biens ou de services, de cession ou concession de droits d'auteur ou de tout autre droit intangible, ou encore comme une vente de bien intangible.
Or, une telle classification présente le risque de voir assimiler les paiements effectués en contrepartie de la mise à disposition, ou de l'utilisation de services en ligne, ou encore la délivrance de produits numérisés, à des redevances, alors même que la délivrance de produits ou services dans le commerce traditionnel ne donne généralement pas lieu à des paiements qualifiés de redevances.

b) En pratique

L'achat, de plusieurs copies électroniques d'un logiciel ou d'un livre, augmente le bénéfice des ventes du fournisseur, alors que l'acquisition d'une version électronique du même produit avec un droit de reproduction peut augmenter :

- le revenu de redevances (dans le cas où l'acheteur est autorisé à «copier» le contenu à des fins commerciales),
- les bénéfices de vente (dans le cas où l'acheteur n'est pas autorisé à copier le contenu à des fins commerciales mais seulement à des fins personnelles),
- les services (dans le cas où l'acheteur a recours aux services de l'auteur pour créer le contenu).

c) Principes

Le revenu de la vente de biens est imposable sur une base nette dans le pays d'origine si le revenu est généré par un établissement stable dans le pays en question. Les redevances et autres types de revenu de placement sont assujettis à une retenue à la source dans le pays d'origine.

3) Régime de TVA applicable aux opérations de commerce en ligne

Ces règles sont issues de la 6e directive européenne du 17 mai 1977 et de la nouvelle directive du 7 mai 2002 qui devra être mise en place par les Etats membres au plus tard le 1er juillet 2003 et relative au régime de la taxe sur la valeur ajoutée applicable à certains services fournis par voie électronique.

<table>
<tr><th>Catégories légales</th><th>Qualification juridique</th><th>Règles applicables</th></tr>
<tr><td rowspan="2">Livraison de biens matériels

La commande en ligne fait l'objet d'une livraison physique.</td><td rowspan="2">Qualification de livraison de biens traditionnelle

Règles habituelles de localisation pour la perception de la TVA : la TVA est due lorsque la livraison a lieu sur le territoire de l'Union européenne.</td><td>Livraison à l'intérieur de l'UE :

▪ Livraison à une personne de l'UE assujettie à la TVA : le fournisseur français ne déclare pas de TVA mais le client doit déclarer la TVA au taux de son pays.

▪ Livraison à une personne non assujettie : le fournisseur français facture le taux de la TVA française à son client. Exception CA > 100 000 euros par an : obligation d'enregistrement auprès des autorités fiscales afin de relever de la TVA locale.</td></tr>
<tr><td>Livraison avec des Etats tiers :

▪ Importation en France de biens en provenance de pays tiers : la TVA est due dans tous les cas.

▪ Exportation vers des pays tiers : aucune TVA française n'est due.</td></tr>
<tr><td>Prestations de services en ligne

La transaction est totalement dématérialisée : par exemple le téléchargement direct sur l'ordinateur du client de livres, disques ou de logiciels.</td><td>Qualification de prestation de services

Est pris en compte le support (électronique) et non la cause (le contenu du livre par exemple) dès lors que l'opération porte sur la livraison de biens dématérialisés. Les conséquences au regard du taux de TVA sont importantes. Ainsi, le taux applicable à l'acquisition d'un livre électronique par voie de téléchargement sera supérieur à celui dont bénéficie la vente d'un livre sur support imprimé.</td><td>Livraison à l'intérieur de l'UE :

▪ Les services sont taxés dans le pays où le prestataire a son établissement. (Dans le cas de plusieurs centres d'activité, on retient le pays de l'établissement le plus concerné par chaque fourniture individuelle).

▪ Exceptions : transferts de droits d'auteur, brevets, marques, dessins et modèles – publicité – services de consultants, avocats – transferts de données / informations – services bancaires, financiers, d'assurance – services de télécommunications. Lorsque le preneur français reçoit les services pour son commerce, il est considéré comme celui qui fournit les services et doit déclarer la TVA, le fournisseur étranger n'étant pas lui-même obligé de la déclarer.

Livraison avec des Etats tiers : Nouvel article 298 sexdecies F du CGI applicable à compter du 1er juillet 2003.

▪ Importation en France de biens en provenance de pays tiers : le nouveau régime prévoit que les services fournis par voie électronique sont considérés pour les besoins de la TVA comme localisés dans l'Union européenne, lorsqu'ils sont fournis par un assujetti établi en dehors de l'Union européenne, en faveur de preneurs établis dans l'Union européenne. Si le preneur est un assujetti, il sera le redevable de la taxe (mécanisme de l'auto liquidation). Si, en revanche, le preneur n'est pas un assujetti, le redevable sera le prestataire établi en dehors de l'Union européenne, lequel sera tenu de se faire identifier aux fins de la TVA dans un seul Etat membre pour s'acquitter de son obligation en tant que redevable de la taxe.

▪ Exportation vers des pays tiers : les entreprises européennes sont dorénavant exonérées de TVA à l'exportation.</td></tr>
</table>

E. Publication sur Internet d'œuvres protégées

Œuvres de l'esprit	Titulaire(s) du droit	Objet de la protection	Droits protégés	Exceptions et fins des droits		
Oeuvres originales portant l'empreinte de la personnalité de leur auteur, protégées « qu'elles qu'en soient la forme, le mérite, la destination ». *Code de la Propriété Intellectuelle (CPI) art. L. 112-1*	• Celui ou ceux sous le **nom** du ou desquels l'œuvre est divulguée. • Cas de **l'œuvre de collaboration** : la création est le concours de plusieurs personnes physiques. • Les droits sont gérés en indivision. • Cas de **l'œuvre collective** : la création est à l'initiative d'une personne physique ou morale qui l'édite et la contribution individuelle des auteurs se fond dans l'ensemble de telle sorte qu'il est impossible d'attribuer à chacun un droit distinct sur l'ensemble réalisé. Auteur =initiateur de la création (cas de toute œuvre audiovisuelle).	1° Les livres, brochures et autres écrits littéraires, artistiques et scientifiques ; 2° Les conférences, allocutions… ; 3° Les oeuvres dramatiques ou dramatico-musicales ; 4° Les oeuvres chorégraphiques… ; 5° Les compositions musicales avec ou sans paroles ; 6° Les oeuvres (…) audiovisuelles ; 7° Les oeuvres de dessin, de peinture, d'architecture… ; 8° Les oeuvres graphiques et typographiques ; 9° Les oeuvres photographiques (…) ; 11° Les illustrations, les cartes géographiques ; 12° Les plans, croquis et ouvrages plastiques (…) ; 13° Les logiciels, y compris le matériel de conception préparatoire ; (…) *CPI art. L. 121-2 extraits*	Droits **moraux :** • Droit à la paternité de l'œuvre, droit au respect de l'œuvre, droit de divulgation, de repentir ou de retrait. *CPI art. L. 121-1* Droits **patrimoniaux** : • Droit de reproduction : droit de communiquer l'œuvre au public par un procédé de reproduction permettant à l'auteur de se faire rémunérer. • Droit de représentation : droit de communiquer l'œuvre de manière indirecte au public. Une autorisation est nécessaire. *CPI art. L. 122-3 et 122-2*	L'auteur ne peut interdire : • les représentations privées et gratuites exclusivement dans un cadre de famille ; • les copies ou reproductions réservées à l'usage privé du copiste et des copies d'un logiciel autres que la copie de sauvegarde ; • les analyses et courtes citations ; • les revues de presse ; • la parodie, le pastiche et la caricature ; • … *CPI art. L. 122-5 extraits*	• L'auteur perd ses droits en cas de transmission par cession, qui doit être expressément mentionnée dans un contrat de cession. • L'auteur reste cependant titulaire des droits qu'il n'a pas expressément cédés en respectant le formalisme prévu par l'article L. 131-3 du CPI.	**Durée** : 70 ans à compter de la mort de l'auteur, à compter de la publication pour les œuvres collectives.

4.1.2. Risques techniques liés à Internet

A. Disponibilité

Le déni de service correspond à l'impossibilité pour l'internaute d'accéder au site (Internet, extranet ou intranet), en raison d'une défaillance technique. Cette défaillance peut avoir une cause interne à l'entreprise (panne du serveur de l'entreprise…), ou externe (problème relatif au réseau, au fournisseur d'accès Internet, à l'hébergeur…).

Une des principales raisons de l'indisponibilité d'un serveur provient d'un trop grand nombre de requêtes, qui peuvent entraîner une dégradation du service (ralentissement des temps d'accès et augmentation des temps de transaction), voire un arrêt total. Il peut s'agir du lancement par les utilisateurs de traitements nécessitant des ressources machines importantes. Il peut également s'agir de l'envoi simultané d'un très grand nombre de messages électroniques (courriels) sur un même serveur, provenant de l'extérieur (spam consistant à une attaque par courriels d'un site Internet).

Dans le cas d'activités de type « B to C » (entreprises vers consommateurs) ou d'un intranet, les conséquences financières pour l'entreprise d'un déni de service peuvent être faibles, voire inexistantes lorsqu'il s'agit de sites éditoriaux, à accès gratuit. Ce n'est pas forcément le cas dans des activités « B to B » (entreprises vers entreprises), faisant le plus souvent appel à un extranet, dont les dommages résultant d'une interruption ou cessation d'activité, peuvent entraîner des difficultés d'exploitation pour l'entreprise fournisseur.

Exemple : une entreprise, offrant des services de place de marché pour les différents acteurs d'un secteur d'activité, peut être amenée à cesser son activité, si elle n'est pas en mesure de rembourser les dommages créés chez ses clients, résultant d'une interruption de service. Comme vu plus haut, le montant des préjudices à rembourser peut être tel, que si l'entreprise n'est pas assurée pour ses activités en ligne, elle pourrait ne pas être en mesure d'y faire face et être amenée à cesser son activité.

Lorsqu'une entreprise sous-traite son activité Internet à un tiers, elle doit prêter une attention particulière aux moyens mis en œuvre par celui-ci pour réduire les risques de déni de service (surveillance de l'activité avec alertes automatiques...) et aux contrats d'assurance couvrant l'activité en cas de dommages.

B. Sécurité des transactions

La sécurité des transactions et des communications concerne les éléments suivants :

- l'authentification : les correspondants doivent pouvoir mutuellement s'assurer de leur identité,
- l'intégrité : le destinataire doit pouvoir s'assurer que les informations reçues n'ont pas été altérées pendant leur transit,
- la confidentialité : seuls les correspondants doivent pouvoir prendre connaissance de l'information échangée,
- la non répudiation : les correspondants ne doivent pas pouvoir nier l'échange d'information.

En fonction des risques liés aux échanges effectués entre l'entreprise et ses clients ou partenaires, les communications devront nécessiter des moyens de sécurité appropriés, par l'utilisation de techniques :

- de chiffrement pour garantir la confidentialité :
  - le chiffrement est une technique permettant de brouiller l'apparence d'un message ou d'un fichier. Il repose sur l'utilisation d'un algorithme (généralement public) et d'une clé (privée). La taille de la clé détermine le nombre de combinaisons possibles,

  - un chiffrement est dit symétrique lorsque seule la clé de chiffrement permet de déchiffrer le message ou le fichier :
    - avantages : rapidité de chiffrement et de déchiffrement,
    - inconvénients : communication et nombre de clés,
  - un chiffrement est dit asymétrique lorsqu'il utilise une paire de clés avec lesquelles ce qui est chiffré par l'une ne peut être déchiffré que par l'autre. Les clés sont liées par une relation mathématique mais ne peuvent être déduites l'une de l'autre,
    - avantages : pallie les inconvénients des chiffrements symétriques (communication et nombre de clés),
    - inconvénients : lenteur, distribution et authentification des clés,
- de signature électronique pour garantir l'authentification :
  - la signature électronique est le moyen permettant au destinataire d'un message de s'assurer de l'identité de son émetteur. En revanche, l'émetteur ne dispose pas de moyen lui permettant de s'assurer de l'identité du destinataire, hormis par chiffrement intelligible uniquement par ce dernier,
  - la signature électronique repose sur les techniques de chiffrement asymétrique : on chiffre un condensé du message avec sa clé privée, et le destinataire vérifiera cette signature en la déchiffrant avec la clé publique de l'émetteur (cette dernière est généralement adjointe au message à l'intérieur d'un certificat numérique),
- de scellement pour garantir l'intégrité :
  - le scellement consiste à adjoindre un sceau numérique à une information afin d'assurer à son destinataire, qu'aucune altération n'a eu lieu pendant son transit. Le sceau est constitué de deux éléments : un condensat et une signature électronique portant sur celui-ci (plutôt que sur l'information elle-même),
  - un condensat est une valeur de petite taille (128 ou 160 bits typiquement) calculée à partir d'un ensemble de données (fichier ou message). En cas d'altération, même d'un bit, le résultat du calcul serait complètement différent. Il est impossible de reconstituer les données d'origine à partir du condensat,
- d'estampillage pour garantir la non répudiation :
  - pour garantir la non répudiation d'une transaction, il faut établir l'identité des acteurs, ainsi que la date et l'heure de la transaction,
  - l'identité des acteurs est établie grâce aux techniques de signature électronique. L'émetteur signe son message et le destinataire en signe l'accusé de réception,
  - la garantie de la date et de l'heure de la transaction passe nécessairement par le recours à un tiers de confiance, qui va estampiller la transaction en datant et en conservant les condensats signés du message et de son accusé de réception.

Depuis la directive européenne du 13 décembre 1999 et sa transposition en droit français, de par l'adoption de la loi du 13 mars 2000 complétée par son décret d'application du 30 mars 2001, la notion de signature électronique bénéficie d'un véritable cadre juridique.

La loi du 13 mars 2000 a défini la notion de signature électronique (comme « une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ») et le décret du 30 mars 2001 a posé les critères pour qu'un procédé de signature électronique soit présumé fiable, jusqu'à preuve du contraire.

Le décret du 18 avril 2002 traite de l'évaluation et de la certification de la sécurité offertes par les produits et les systèmes des technologies de l'information. Un arrêté du 31 mai 2002 fixe les règles relatives à la reconnaissance de la qualification des prestations de certification électronique et à l'accréditation des organismes chargés de l'évaluation.

L'écrit sur support électronique a alors la même force probante que l'écrit sur support papier, bien que dans le cas de la signature électronique non sécurisée, la fiabilité du procédé d'identification doit être prouvée (ce qui en pratique peut nécessiter le recours à une expertise).
Sauf dispositions légales contraires, en matière commerciale, tous les modes de preuve sont admissibles. L'écrit n'a donc pas une force probante privilégiée. Le juge a un pouvoir souverain d'appréciation. Par exemple, il tient compte des pratiques courantes d'échange de télécopie ou de télex pour des passations de commandes ou la conclusion de contrats.

La jurisprudence admet que les parties puissent contractuellement renoncer à l'obligation de prouver par écrit et reconnaissent la validité de certains moyens de preuve en signant une convention sur la preuve. En matière d'échanges électroniques, les entreprises peuvent conclure des accords spécifiques qui sont également des conventions sur la preuve.

Les échanges avec le grand public sont gérés différemment, puisque le juge est en effet lié par les règles de preuve du Code civil. Lorsqu'un écrit est exigé (par exemple, une transaction supérieure à 750 euros), il ne peut accepter d'autres modes de preuve, sauf à relever de l'une des exceptions prévues par la loi, par exemple l'impossibilité matérielle et la copie fidèle et durable.

Dans les systèmes de gestion électronique de document où l'écrit est préexistant à la dématérialisation, la valeur probante du document électronique dépendra du sort réservé à l'original. L'entreprise devra alors mettre en place une méthode de preuve sur la base de la copie en fonction du sort de l'original écrit. Ce dernier peut soit avoir été conservé tel que (archivage papier) ou détruit après avoir fait l'objet d'une reproduction sur un support fidèle et durable (micro-fiche par exemple).

Dans le cas des échanges de données informatisées, il n'existe aucun écrit préalable, puisque le document naît sous une forme électronique et se matérialise sous la forme d'un document écrit, à l'issue de l'échange. En cas de litige, la présentation d'un tel document ne peut alors relever des exceptions prévoyant la nécessité d'un écrit préexistant (copie fidèle et durable notamment). En revanche et sous réserve de l'appréciation souveraine des juges, l'impossibilité matérielle d'obtenir un écrit peut valoir dispense.

C. Intrusions

Les intrusions sont des accès extérieurs et non autorisés à l'environnement Internet de l'entreprise. Elles peuvent être le fait de personnes physiques qui essaient de forcer un système donné, ou d'automates dont l'objet est de détecter les sites qui présentent des failles sur Internet.

Les intrusions sont menées avec deux objectifs principaux : accéder aux données de l'entreprise (le plus souvent il s'agit d'intrusions effectuées « manuellement », au coup par coup) ou utiliser les ressources machine du système (un site est utilisé pour archiver des fichiers à l'insu de son propriétaire ou pour attaquer un autre site et ainsi masquer l'identité de l'attaquant). En fonction du degré de sensibilité des données gérées et des risques associés aux activités Internet, l'entreprise aura intérêt à mettre en place une politique sécurité adaptée.

Les systèmes de détection d'intrusions (IDS : Intrusion Detection Systems) cherchent à automatiser le repérage d'activités suspectes annonciatrices ou révélatrices d'une possible violation de la sécurité de l'entreprise. La technique repose sur l'observation par un programme de l'ensemble du trafic qui transite en un point jugé névralgique. Les solutions actuelles sont très majoritairement logicielles mais ont de plus en plus de difficultés à prendre en compte un trafic de données croissant, permis par les liaisons haut débit. C'est pourquoi, des solutions matérielles se développent actuellement pour répondre à cet inconvénient.

D. Infections virales

Un virus est un programme hostile dont l'objectif est d'infecter les fichiers d'un système (principalement les fichiers exécutables), en y insérant une copie de lui-même. Il peut en résulter des dommages au niveau du système d'exploitation, des programmes…, responsables de dysfonctionnements divers, d'effacement ou aspiration des données, etc.

Il existe plusieurs types de virus dont les principaux sont les suivants :

- les macro-virus : ils s'attaquent le plus souvent aux fonctions de macro-commandes des logiciels bureautiques,
- les vers : ils se développent sur le réseau et dans le système d'exploitation,
- les bombes logiques : elles se déclenchent à une date donnée ou au lancement d'une commande déterminée,
- les canulars : il s'agit de courriers électroniques faisant croire que l'ordinateur est infecté par un virus et demandant à l'utilisateur de supprimer des programmes nécessaires au fonctionnement du système d'exploitation,
- le cheval de Troie : il s'agit d'un programme placé à l'intérieur d'un autre, destiné à désactiver les systèmes de protection ou à dérober les mots de passe et faciliter une intrusion externe,
- les virus polymorphes : ils sont rendus indétectables car ils modifient automatiquement leur apparence en intégrant dans leur code une fonction de cryptage dont la clé de chiffrement est différente à chaque duplication. La fonction de déchiffrement contient un nombre aléatoire d'instructions ayant pour objectif de rendre le virus indétectable par un antivirus.

Les infections virales se transmettent au moyen de la messagerie électronique, le virus étant intégré directement au niveau du message (cas assez rare), ou au niveau de la pièce attachée au message. Dans le premier cas, le simple fait d'ouvrir le message déclenche l'exécution du virus (si aucun anti-virus n'est installé), dans le second, le déclenchement intervient à l'ouverture du fichier joint. Plus traditionnellement, ils peuvent se dissimuler dans un programme sur disquette ou CD-ROM.

Il est important que toute entreprise mette en place une politique de prévention et de traitement des virus, en prenant en compte les endroits stratégiques que sont les postes de travail, les serveurs de fichiers, les serveurs de messagerie et les passerelles Internet.
Certains antivirus étant plus efficaces que d'autres pour lutter contre certains types de virus, il est conseillé d'installer des antivirus à chacun des endroits stratégiques, de marque différente pour avoir la plus grande couverture possible :

- Antivirus sur passerelle Internet
  - Point d'entrée d'Internet dans l'entreprise, la passerelle Internet doit avoir des antivirus couplés avec le pare-feu chargé notamment de filtrer l'accès aux machines du réseau. L'antivirus est alors installé sur une machine dédiée et analyse l'ensemble du flux entrant de données smtp (courriels), http (web), ftp (transfert de fichiers), avant de le rendre au pare-feu qui l'achemine vers son destinataire. Des mécanismes de filtre peuvent également bloquer des courriels en fonction de mots-clés contenus dans le sujet ou le corps du message.
  - L'inconvénient d'un tel dispositif est d'alourdir le traitement des échanges avec Internet, en particulier lorsqu'il s'agit des flux http. Pour remédier à ce problème, il est possible d'installer l'antivirus sur un proxy, ordinateur entre un réseau privé et Internet, dont la fonction de cache permet de minimiser les temps de traitement.

- Antivirus sur serveurs de messagerie
  - En plus d'un antivirus installé sur la passerelle Internet, il est recommandé d'installer un antivirus sur le serveur de messagerie. En effet, un virus non détecté par la passerelle antivirus pourra l'être par le serveur de messagerie, s'il provient d'un éditeur différent (d'où l'importance de choisir des fournisseurs d'antivirus différents).
  - Ce type d'antivirus est également justifié par le fait que les utilisateurs d'une entreprise utilisent de plus en plus une messagerie personnelle « Internet », c'est-à-dire accessible à travers un navigateur et donc le protocole http. Un antivirus installé sur le serveur de messagerie détectera le virus contenu dans un courrier électronique s'il est renvoyé par le logiciel de messagerie.

- Antivirus sur les postes de travail
  - Il est nécessaire d'installer un antivirus fichier qui analysera tous les fichiers présents sur le disque ainsi que tous les fichiers obtenus par messagerie ou téléchargés sur le web. Pour être efficace, il faut que les logiciels soient mis à jour régulièrement et automatiquement.
  - L'antivirus ne doit pas pouvoir être désactivé ou désinstallé par l'utilisateur de la machine, et toute nouvelle machine installée sur le réseau devra être systématiquement protégée par l'installation de l'antivirus.

- Antivirus sur les serveurs de fichiers
  - Un antivirus fichier devra être installé, de préférence d'un éditeur différent de celui installé sur les postes de travail. Les serveurs de fichiers mettant à disposition des ressources partagées et communes sont particulièrement sensibles aux virus qu'ils peuvent propager très rapidement à l'ensemble de l'entreprise.
  - Tous les fichiers accédés devront être analysés lors de l'ouverture et écriture.

4.2. Mise en œuvre des contrôles juridiques et techniques dans la mission d'audit

Le caractère significatif ou non de l'activité Internet de l'entreprise auditée, la complexité et la diversité des fonctionnalités, ainsi que les caractéristiques des produits ou services offerts, nécessitent une analyse adaptée des risques juridiques et techniques qui en résultent.

Concernant l'analyse des risques techniques, elle peut être facilitée lorsque l'entreprise souscrit à des services de tests de vulnérabilité et de performances. Ces services sont proposés la plupart du temps sous la forme de rapports en ligne, mis à jour régulièrement, auxquels l'entreprise peut accéder en permanence pendant toute la durée du contrat.

5. THEME 5 : LES RISQUES LIES A L'EXISTENCE D'UN PROJET INFORMATIQUE

Ce dossier thématique permet au commissaire aux comptes de mieux appréhender les risques liés à l'existence d'un projet informatique dans une entreprise. Il vient en complément des informations présentées sur ce sujet dans le chapitre « Méthodologie », « Incidence de l'environnement informatique sur le risque inhérent ».

La notion de projet informatique ne s'applique pas uniquement aux entreprises de grande taille. Le remplacement d'un système d'information par un autre doit être considéré comme un projet informatique et concerne par conséquent toutes les entreprises.

La réussite d'un projet est liée à la maîtrise des budgets et du calendrier. Les projets informatiques modifiant durablement et en profondeur l'entreprise, le commissaire aux comptes doit être vigilant lorsqu'il intervient dans un tel environnement.

Les domaines sensibles d'un projet informatique sont les suivants :

- prise de connaissance de l'étude préalable et analyse de son adéquation par rapport :
  - à la stratégie de l'entreprise,
  - aux besoins des utilisateurs,
  - à l'existant (logiciel, moyens, infrastructure…),
  - aux bonnes pratiques,
- prise de connaissance de la conception détaillée et analyse de son adéquation par rapport :
  - à l'étude préalable,
  - à l'ergonomie de l'outil développé,
  - à la prise en compte du contrôle interne et de la sécurité (mots de passe, profils, piste d'audit…),
  - aux mesures prises pour assurer l'intégrité des traitements, la disponibilité de l'application,
- prise de connaissance de la phase de test et de déploiement et analyse pour vérifier sa pertinence, par rapport :
  - aux jeux d'essais qui doivent correspondre aux activités de l'entreprise et couvrir les principaux cas,
  - à l'exploitation de la solution mise en place,
- analyse de la conduite de projet,
- analyse de la conduite du changement.

5.1. Présentation d'un projet informatique

5.1.1. Définition d'un projet informatique

Selon l'AFNOR, « un projet est une démarche spécifique qui permet de structurer méthodiquement et progressivement une réalité à venir. Un projet est défini et mis en œuvre pour élaborer une réponse au besoin d'un utilisateur, d'un client ou d'une clientèle, et il implique un objectif et des actions à entreprendre avec des ressources données » (Norme X50-106).

Les caractéristiques d'un projet sont les suivantes :

- limité dans le temps : un projet est mené par rapport à un calendrier,
- unique : s'il existe de nombreux projets analogues ou similaires, les projets ne sont pas identiques en raison des évolutions technologiques et des spécificités organisationnelles d'une entreprise à l'autre,
- pluridisciplinaire : la conduite de projet requiert des compétences techniques, administratives, financières, sociales et juridiques.

5.1.2. Principales causes d'échec d'un projet informatique

A. Absence de cahier des charges et documentation insuffisante

Le cahier des charges est un document rédigé au début du projet. Il contient une description des fonctionnalités à réaliser, des performances et des conditions d'exploitation attendues par le système, des principales contraintes à respecter pour satisfaire les besoins exprimés. Si le cahier des charges doit être le plus détaillé possible, il ne peut cependant jamais être totalement exhaustif.

B. Absence de motivation des parties prenantes au projet

La motivation est une donnée indispensable à la réussite d'un projet. Les échecs peuvent être le fait :

- d'une absence de soutien de la direction,
- d'une démotivation de la maîtrise d'œuvre dont le travail n'est pas défini précisément ou qui est soumise à des pressions trop importantes,
- d'un manque d'implication des utilisateurs aux différentes phases du projet, en particulier à la phase de conception.

L'absence de motivation résulte souvent d'un manque de communication entre les différents intervenants.

C. Faiblesses dans la gestion de projet

Les faiblesses dans la gestion de projet concernent les domaines suivants :
- les méthodes d'estimation et de planification des travaux,
- la gestion des moyens disponibles,
- la communication entre les parties,
- la gestion des compétences,
- etc.

Les questions relatives à l'organisation et au contrôle interne sont généralement délaissées au profit des aspects techniques. La problématique du contrôle interne est souvent traitée a posteriori, ce qui implique une période de transition pendant laquelle le niveau de contrôle est plus faible : les états de gestion et les procédures de contrôle sont souvent modifiés avec la mise en place d'un nouveau système d'information.

5.1.3. Conditions de réussite d'un projet informatique

A. Réaliser un diagnostic de la situation actuelle

La connaissance du fonctionnement de l'entreprise est une condition importante à la réussite du projet informatique, nécessaire à la définition du cahier des charges et à la mise en place d'une organisation projet adaptée aux caractéristiques de l'entreprise. Une mauvaise identification des besoins et des objectifs à atteindre au départ du projet peut conduire les responsables du projet à effectuer des choix par défaut en cours de projet, générateurs de dysfonctionnements pérennes.

B. S'appuyer sur une méthodologie efficace et conduire le changement

L'utilisation d'une méthodologie et la maîtrise des concepts et des outils de gestion de projet ne sont pas suffisantes à la réussite du projet. Il convient d'associer et d'impliquer la totalité des acteurs concernés par la mise en place d'actions de conduite du changement. Changer les mentalités demeure le préalable à toute action et repose sur la capacité des individus à accepter le changement. L'état d'esprit des équipes est la principale condition de réussite.

5.1.4. Etapes d'un projet en système d'information

A. Intérêt du découpage d'un projet en phases

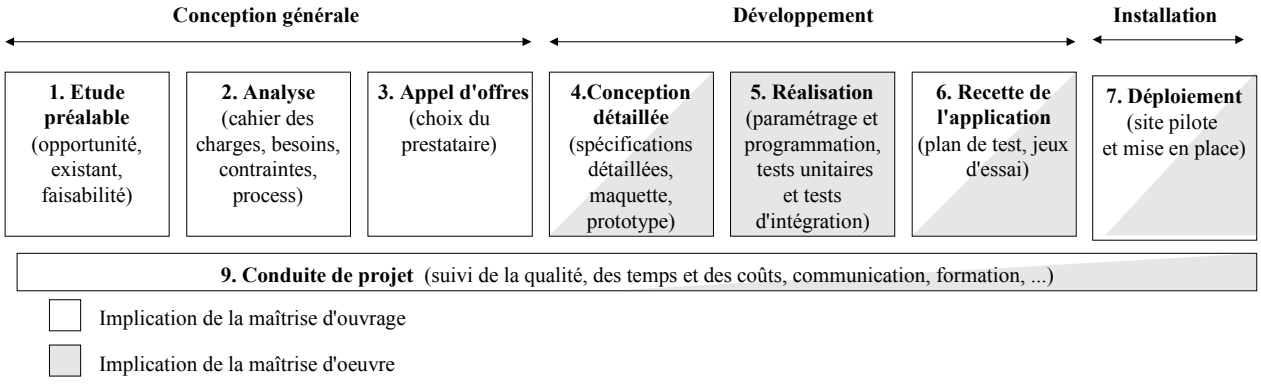
La structuration du projet en phases contribue très sensiblement à améliorer les processus d'estimation, de planification et de suivi, en réduisant les risques de dérives en termes budgétaire et de calendrier.

La maîtrise du projet passe par le suivi et la mise à jour régulière du calendrier général, en fonction de l'avancement des différents travaux à mener. Des actions rapides pourront être entreprises en cas de dérapage de l'une des phases, évitant la dérive de l'ensemble du projet.

Un responsable est affecté à chacune des phases du projet : il est chargé d'atteindre les objectifs fixés dans la planification initiale, en termes de coûts et de délais, en isolant les tâches critiques et en identifiant les acteurs et ressources nécessaires à leur réalisation.

B. Présentation des phases et étapes d'un projet

Traditionnellement, un projet peut faire l'objet du découpage suivant :



- La phase de conception générale consiste à initier le projet et à en définir son périmètre. Elle est composée d'une étude préalable visant à déterminer les objectifs du projet et la capacité de l'organisation de le mener à bien. Intervient ensuite une étape d'analyse qui, au travers de l'élaboration du cahier des charges, permet de spécifier les besoins nécessaires à l'appel d'offres et de choisir le maître d'œuvre et/ou le produit le plus adapté aux besoins.

- La phase de développement correspond à la réalisation par la maîtrise d'œuvre du système spécifié par la maîtrise d'ouvrage. Au cours de la première étape de conception détaillée, les deux parties travaillent en commun et valident les solutions proposées. La maîtrise d'œuvre réalise ensuite les développements devant faire l'objet d'une validation par la maîtrise d'ouvrage.

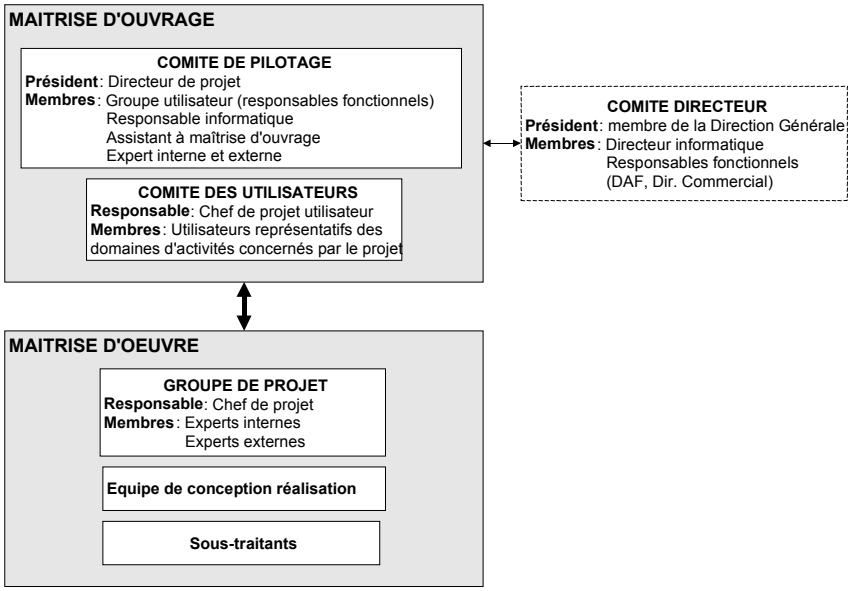
- La phase d'installation consiste à la mise en place du système sur l'ensemble des sites concernés.

- La fonction de conduite de projet s'étend pendant toute la durée du projet et vise à en assurer la maîtrise, par un pilotage des différentes étapes. Elle se traduit par un contrôle des coûts, des délais et de la qualité, mais aussi par des actions de conduite du changement et de formation.

5.1.5. Acteurs d'un projet

La conduite d'un projet implique l'engagement de deux parties : le client ou « maître d'ouvrage » et le fournisseur ou « maître d'œuvre ». Le comité directeur (direction générale) initie le projet et définit les orientations stratégiques.

Le schéma ci-dessous présente pour exemple, l'organisation type de la gestion de projet d'une entreprise de grande importance.



A. Le comité directeur

Le comité directeur est un comité permanent qui définit la politique informatique de l'entreprise. Dans le cadre d'un projet, le comité directeur :

- initie le projet et définit les orientations au regard des objectifs stratégiques de l'entreprise,
- définit le périmètre fonctionnel du système,
- met en place le comité de pilotage auquel il demande l'élaboration du budget,
- valide le budget et décide du démarrage des travaux.

Dès la fin de l'étude préalable, le comité directeur n'intervient plus directement dans la vie du projet et confie ce rôle au comité de pilotage. Dans les petites et moyennes entreprises, le comité directeur n'existe pas, il est remplacé par le comité de pilotage.

B. La maîtrise d'ouvrage

La maîtrise d'ouvrage est souvent la direction générale ou une direction opérationnelle, pour le compte de laquelle le projet est réalisé. La maîtrise d'ouvrage est impliquée dans le projet en tant que futur utilisateur du système et donneur d'ordres. Son organisation est fonction de la taille du projet, mais elle est souvent constituée par le comité de pilotage et le comité des utilisateurs.

1) Le comité de pilotage

Il est l'organe directeur de la maîtrise d'ouvrage et est créé par le comité directeur à qui il rend compte de l'évolution du projet. Il est présidé par un directeur de projet. Il est aussi composé des représentants opérationnels (groupes utilisateurs) concernés par la nouvelle application, du responsable informatique de la société, de l'assistant à maîtrise d'ouvrage, d'experts internes ou externes.

Les attributions du comité de pilotage sont les suivantes :

- lancement du projet caractérisé par les objectifs, les finalités, les critères de qualité et l'arbitrage des moyens à mettre en œuvre,
- définition des choix stratégiques d'architecture et des orientations en matière de sécurité et de droits d'accès,
- conduite du changement et mise en œuvre intégrant notamment les plans de communication et de formation,
- management du projet correspondant au suivi des échéances, des risques et du contrôle qualité.

2) Le comité des utilisateurs

Il est constitué de tous les utilisateurs représentatifs des domaines d'activité concernés par le projet. Il est important de disposer d'une réelle participation de ses membres durant le déroulement du projet.
Le comité des utilisateurs est piloté par un chef de projet utilisateur. Ses attributions sont les suivantes :

- expression détaillée des besoins et des règles de gestion,
- validation des solutions / maquettes présentées par l'équipe projet,
- participation aux tests du système informatique,
- participation aux actions de formation,
- réception définitive du logiciel.

C. La maîtrise d'œuvre

La maîtrise d'œuvre met en place ou développe une solution conforme aux spécifications validées, dans des conditions de coût, de délais et de qualités, fixées par la maîtrise d'ouvrage. D'une manière générale, la maîtrise d'oeuvre est représentée par le responsable informatique de l'entreprise et/ou par un prestataire de service de type société de services informatiques (SSII), sélectionné par la maîtrise d'ouvrage.

La maîtrise d'œuvre est organisée autour d'un groupe de projet, son organe de décision. Ce groupe a pour mission de produire l'ensemble des travaux relevant des attributions de la maîtrise d'œuvre. Il est généralement constitué de la façon suivante :

- un chef de projet qui assure la fonction d'animation,
- des ingénieurs de conception et de réalisation,
- un responsable qualité et méthodes chargé de la planification,
- éventuellement des experts.

Le groupe de projet a pour principale tâche de gérer les équipes de développement et/ou de paramétrage, interne ou externe. Il organise l'assurance qualité et suit l'avancement et la consommation des ressources du projet. Organe de décision de la maîtrise d'œuvre, il communique avec la maîtrise d'ouvrage au travers de réunions ou de tableaux de bord permettant le pilotage du projet.

La maîtrise d'œuvre est également constituée d'équipes de conception et de réalisation qui paramètrent, programment et développent le système d'information cible. Elle peut être sous-traitée à un prestataire externe. Dans ce cas, il est indispensable qu'une personne de l'entreprise fasse partie du groupe de projet.

La maîtrise d'œuvre assure les fonctions suivantes :
- identifie et planifie les tâches à réaliser,
- détermine les moyens humains et matériels nécessaires à la conduite du projet,
- effectue les travaux d'étude et de réalisation,
- fournit au directeur de projet les logiciels testés,
- rend compte au directeur de projet de l'avancement du projet et lui soumet les éléments à valider.

Elle n'est responsable que dans la limite de son périmètre d'intervention, mais a un devoir de conseil et d'alerte des risques pouvant résulter des orientations prises par le maître d'ouvrage.

D. Fonctions respectives et relations entre les acteurs du projet

Un des principaux facteurs de succès d'un projet est la qualité de la relation entre la maîtrise d'ouvrage et la maîtrise d'œuvre. De nombreux dysfonctionnements proviennent d'un manque de confiance entre ces deux acteurs.

La confiance repose notamment sur les principes suivants :
- définition claire et précise des rôles respectifs de la maîtrise d'ouvrage et de la maîtrise d'œuvre,
- projet doté de structures décisionnelles, calendrier de réunions (fréquence, thèmes abordés, participants), existence de modalités d'arbitrage en cas de conflit,
- transparence et communication à travers la mise en place de réunions de travail et de points d'avancement.

La maîtrise d'ouvrage doit rester forte et conserver l'orientation stratégique du projet, même si la maîtrise d'œuvre joue un rôle de conseil.

5.2. Risques liés à l'existence d'un projet informatique

La conduite de projet suppose sa maîtrise à travers son pilotage, la définition et le respect d'un plan d'assurance qualité, la conduite du changement et la communication. L'analyse de ces points permet d'évaluer le niveau de risque que présente un projet informatique en cours.

5.2.1. Pilotage du projet

Un projet doit faire l'objet d'une définition précise par la maîtrise d'ouvrage en terme d'objectifs, de délais, de coûts et de qualité. Ces informations sont indispensables au pilotage d'un projet.

5.2.2. Suivi des délais

La définition du calendrier détaillé des actions à réaliser consiste à évaluer chacune d'elles en termes de charge et de durée :

- la charge représente la quantité de travail nécessaire à la réalisation d'une action, indépendamment du nombre de personnes. Elle s'exprime généralement en jour/homme,
- la durée est fonction du nombre de ressources affectées à une action.

Les actions à réaliser sont positionnées les unes par rapport aux autres en fonction des priorités identifiées, pour permettre un suivi des tâches et déterminer le chemin critique. Une représentation schématique de l'enchaînement des tâches est souvent utilisée par la maîtrise d'œuvre pour faciliter le pilotage du projet. La maîtrise d'oeuvre est responsable du respect des délais, en affectant les ressources nécessaires à une tâche donnée et en effectuant les arbitrages dans le cadre du budget initial.

5.2.3. Suivi des coûts

La maîtrise d'ouvrage est en charge de la gestion budgétaire du projet. Elle doit mettre en place des outils de suivi et de prévisions, à utiliser pendant toute la durée du projet, pour limiter le risque de dérapage financier.

A. Principe de détermination d'un budget

Lors de l'étude préalable, la maîtrise d'ouvrage définit le budget à allouer au projet. L'estimation doit tenir compte des dérapages possibles et déterminer le plafond budgétaire maximum à ne pas dépasser. Le risque est de sous-estimer le budget par optimisme ou par sous-estimation des tâches nécessaires au bon déroulement d'un projet (documentation, recette, formation...).

Une mauvaise estimation du budget peut avoir des conséquences directes sur le respect des objectifs assignés au projet ou sur la qualité du système d'information. La qualité des prévisions joue un rôle important dans le succès du projet et est un préalable à la gestion des priorités.

B. Méthodes d'estimation des coûts

Les méthodes d'estimation des coûts d'un projet sont nombreuses. Les méthodes suivantes peuvent être utilisées :

- modèle analytique : le coût du projet est calculé à partir de l'estimation individuelle des composants et des tâches,
- estimations faites par plusieurs experts : un coordinateur réalise une synthèse des estimations réalisées par plusieurs experts,
- coût estimé par comparaison : rapprochement avec un projet présentant des similitudes. Les différences sont mises en évidence et les écarts sont pris en compte,
- meilleure offre du marché : l'estimation est basée sur les réponses faites par des fournisseurs à un appel d'offres.

L'estimation des coûts permet à la maîtrise d'œuvre et à la maîtrise d'ouvrage le suivi budgétaire du projet.

C. Pilotage des coûts

Le pilotage des coûts doit permettre de respecter le budget initial pendant toute la durée du projet. Il peut être possible de réviser les conditions de départ, selon les modalités suivantes :

- un avenant budgétaire est accordé par le maître d'ouvrage, augmentant les ressources existantes,
- une redistribution interne entre lignes budgétaires (à budget global constant) est acceptée par la maîtrise d'ouvrage,
- une modification nécessaire du cahier des charges est décelée par la maîtrise d'œuvre et acceptée par la maîtrise d'ouvrage.

L'objectif du pilotage des coûts est de détecter rapidement les écarts entre les prévisions et le réalisé et d'en analyser les raisons. Le budget doit pour cela être décomposé en lignes budgétaires correspondant aux différentes tâches identifiées dans le calendrier détaillé (lotissement des actions à mener). Pour un pilotage efficace des coûts et une détection précoce des éventuels dérapages, le budget ne doit pas être défini à un niveau trop général ou à un niveau trop détaillé. L'utilisation d'outils de gestion de projet est souvent nécessaire pour faciliter la remontée et la consolidation des informations.

5.2.4. Suivi de la qualité

A. Critères de qualité

Les critères de qualité généralement utilisés par la maîtrise d'ouvrage sont les suivants :

- la fiabilité : les mêmes traitements doivent produire les mêmes résultats et être conformes au cahier des charges,
- l'intégrité : la sécurité de l'accès aux données nécessite la mise en place d'une gestion d'accès et de mots de passe,
- l'efficacité : les temps de réponse doivent être adaptés aux volumes traités,
- la maintenance : un système d'information nécessite une administration permanente, qu'il s'agisse de la correction des anomalies ou de la mise à jour des programmes,
- l'adaptabilité : la capacité de l'application à faire l'objet d'évolutions est une préoccupation forte des équipes informatiques. L'indépendance d'une application par rapport à un environnement matériel ou à un système d'exploitation peut être un élément important dans la stratégie informatique d'une entreprise,
- le confort : l'application doit être simple d'utilisation pour limiter les erreurs de traitements.

Le choix des facteurs de qualité dépend essentiellement des caractéristiques de l'application, de sa durée de vie, de l'environnement d'exploitation, de son importance dans le fonctionnement de l'entreprise, etc.

B. Pilotage de la qualité

Piloter la qualité requiert la mise en place d'instruments d'observation et de mesure dans les domaines suivants :

- mesure de cohérence sur les objectifs : le principe est la mesure du respect des objectifs du projet tout au long de son déroulement. Par exemple, lors de la phase d'expression des besoins, la cohérence des objectifs avec les besoins des utilisateurs doit être vérifiée. Cette analyse permet d'estimer la probabilité de réussite du projet,

- mesure de conformité aux normes : il est nécessaire de mettre en place un dispositif de vérification et de validation de la présence de normes et méthodologies, pour vérifier la conformité des actions menées,
- mesures de performances : l'objectif est de déterminer le niveau d'efficacité, de fiabilité et de retour sur investissement du système proposé compte tenu des objectifs choisis. Les mesures de la performance se répartissent sur l'ensemble des phases du cycle de développement d'un produit. Ces mesures sont en général plus nombreuses dans la phase de réalisation et de mise en oeuvre. Elles répondent à des critères de taille du projet, de nombre de défauts, de structure de données,...

CHAPITRE 3 : LES TECHNIQUES D'AUDIT ASSISTEES PAR ORDINATEUR

1. INTRODUCTION

Ce chapitre complète la méthodologie décrite dans les chapitres précédents et traite des conditions de mise en œuvre des techniques d'audit assistées par ordinateur, utilisables par le commissaire aux comptes dans le cadre de ses contrôles substantifs.

Les techniques d'audit assistées par ordinateur sont à la disposition du commissaire aux comptes pour analyser les données de l'entreprise, parallèlement aux techniques de sondages sur les procédures :

- elles sont utilisées pour quantifier un risque ayant fait l'objet d'une évaluation de niveau modéré ou élevé, sachant qu'il est fortement déconseillé d'entreprendre une analyse de données sans étude du contrôle interne préalable,
- elles permettent de vérifier les calculs effectués par les systèmes de l'entreprise, mais également d'effectuer d'autres opérations de gestion sur les données :
  - rapprochement ligne par ligne entre différents fichiers,
  - recherche de doublons,
  - extraction d'anomalies d'un fichier.

Ces techniques s'appuient sur des fichiers contenant les données extraites du système d'information de l'entreprise et se différencient des notions :

- d'automatisation des dossiers de travail,
- d'informatisation du processus d'élaboration des comptes,
- de requêtes effectuées directement dans les bases de données du système d'information de l'entreprise.

2. PRATIQUE DES TECHNIQUES D'AUDIT ASSISTEES PAR ORDINATEUR

2.1. Introduction

Le traitement de données informatisées n'est plus réservé aux seules entreprises capables d'investir dans des systèmes coûteux. En effet, les systèmes de traitement sont désormais accessibles aux petites et moyennes entreprises.

Face au volume considérable de données et à la complexité de plus en plus accrue des systèmes d'information utilisés par les entreprises, le commissaire aux comptes doit faire face aux exigences suivantes :

- effectuer les tests répondant aux objectifs de l'audit,
- transformer des masses de données en informations : ceci passe par l'utilisation des données disponibles sur l'ensemble du système d'information pour contrôler les comptes,
- automatiser les travaux d'audit habituellement effectués manuellement, en prenant en compte le fait que la récupération de ces données et leur mise en forme sont entièrement automatisées dans les systèmes de l'entreprise.

2.2. Techniques d'audit assistées par ordinateur dans le cadre de la mission d'audit

La norme CNCC 2-302 « Audit réalisé en milieu informatisé » précise que :

- un environnement informatique peut avoir une influence sur « la conception et l'exécution de tests de procédures et de contrôles substantifs nécessaires en la circonstance pour atteindre l'objectif de l'audit »,
- « le traitement et l'analyse de grandes quantités de données par l'informatique peuvent permettre au commissaire aux comptes d'appliquer des techniques ou d'utiliser des outils d'audit informatisés généraux ou spécifiques pour l'exécution de ses contrôles ».

2.3. Techniques d'audit assistées par ordinateur dans le cadre de missions contractuelles

Les techniques d'audit assistées par ordinateur peuvent également être utilisées dans le cadre de missions contractuelles (fiabilisation du système d'information, analyse de populations pour les besoins marketing, etc.).

L'objectif est fixé contractuellement, par exemple :

- réaliser une analyse statistique des populations de clients sur des critères marketing,
- rapprocher les données émises par une application des données reçues dans une autre pour vérifier une interface,
- etc.

Qu'il s'agisse de la mission d'audit ou d'une mission contractuelle, les principes restent les mêmes :

- contrôle de cohérence des données fournies,
- traçabilité des traitements effectués,
- documentation des travaux,
- élaboration d'un rapport de fin de mission.

2.4. Avantages des techniques d'audit assistées par ordinateur

Ces techniques sont de nature à :

- permettre l'obtention d'éléments probants dans un environnement dématérialisé,
- dépasser le stade du sondage dont l'exploitation est toujours délicate compte tenu des difficultés de mise en œuvre et de la non exhaustivité des contrôles,
- identifier systématiquement toutes les anomalies répondant aux critères de sélection et / ou de calcul retenus,
- procéder à des traitements par simulation pour mesurer l'impact de changements de méthode,
- aborder des contrôles fastidieux et complexes sur des populations nécessitant un nombre de calculs difficilement réalisables par une approche manuelle.

2.5. Technique d'audit standard et technique d'audit spécifique

Le commissaire aux comptes doit choisir entre mettre en place une série de tests standards qu'il a pu expérimenter sur d'autres clients (ayant des problématiques analogues), ou concevoir de nouveaux tests adaptés à chaque situation rencontrée. Cette dernière solution reste évidemment plus coûteuse en termes de temps et de ressources.

Il convient de distinguer entre trois approches possibles : la technique d'audit standard, la technique d'audit spécifique et la technique d'audit intermédiaire. Ces approches ont toutes pour objectif de mettre à la disposition du commissaire aux comptes un outil opérationnel.

2.5.1. La technique d'audit standard

Cette solution consiste à développer une série de tests applicables au plus grand nombre d'entreprises. Ce choix entraîne des contraintes importantes sur les données en entrée qui doivent toujours être présentées dans le même format.

Or, les données issues des systèmes d'information des clients sont différentes. Les champs de type « date », par exemple, peuvent être stockés sous des formats différents : jj/mm/aaaa, aaaa/mm/jj, mm/jj/aaaa, etc. Il est donc nécessaire d'adapter les données de l'entreprise à la structure des programmes. Cette étape préliminaire est indispensable et peut s'avérer dans certains cas fastidieuse en fonction du nombre de modifications à apporter aux données.

Il convient également d'évaluer la capacité des entreprises à fournir, d'une année à l'autre, des fichiers de même structure. Cette solution s'applique généralement à des contrôles simples tels que la sélection statistique, la vérification d'un calcul d'indemnités de départ à la retraite, etc.

2.5.2. La technique d'audit spécifique

Cette solution consiste à développer pour chaque entreprise une série de tests adaptés à la structure de ses données. L'application développée récupère les données des systèmes amont (paie, stocks, comptabilité, etc.), puis les transforme pour les adapter aux programmes de travail d'audit et enfin les charge dans des bases de données réservées aux tests. Le commissaire aux comptes peut ainsi dérouler ses tests à tout moment, sans solliciter les ressources de l'entreprise à chaque intervention, pour l'extraction des fichiers par exemple.

Les avantages de cette solution sont :

- une grande souplesse dans l'intervention et un suivi régulier des postes clés sensibles, tels que les stocks, puisque les données sont stockées dans les bases de données réservées aux tests,
- un gain de temps important puisque les programmes ne sont développés qu'une seule fois et exécutés de multiples fois.

En revanche, cette solution exige un investissement initial important pour développer tous les programmes et mettre en place le système de récupération et de sauvegarde des données. Elle s'applique en conséquence aux missions importantes dans un environnement informatique relativement pérenne.

2.5.3. La technique d'audit intermédiaire

Cette solution consiste à développer des petits programmes par thème (paie, stocks, ventes, achats, etc.), sans tenir compte dans un premier temps du format des données clients. Ces programmes seront ensuite adaptés à la problématique du client et à la nature des données à intégrer.

Par exemple pour la paie, les tests les plus utilisés sont :

- la recherche de doublons sur les noms des employés, sur les matricules des employés, sur le numéro d'identification (numéro de sécurité sociale), sur les numéros de compte bancaire,
- le rapprochement entre les employés ayant une fiche de paie et ceux apparaissant sur les listes tenues au service du personnel,
- la liste des employés sans numéro d'identification (sécurité sociale),
- le rapprochement entre les employés qui apparaissent dans le fichier des paiements et ceux qui n'apparaissent pas dans la paie,
- la liste des enregistrements pour lesquels le montant net sur les fiches de paie diffère du montant payé par la banque au-delà d'un seuil donné,
- la sélection aléatoire d'employés.

Cet éventail de tests permet au commissaire aux comptes de couvrir les domaines sensibles de la paye et peut être appliqué aux entreprises quelle que soit leur taille.

2.6. Cas des progiciels de gestion intégrés

Les progiciels de gestion intégrés (PGI ou ERP, Enterprise Ressource Planning) sont des produits qui assurent la gestion globale des activités de l'entreprise. Ces progiciels traitent notamment des données qui sont nécessaires à l'établissement des comptes et à l'information financière.

Lors de leur mise en place, les PGI sont adaptés à l'entreprise en utilisant des tables de paramétrage et des développements spécifiques. Cependant, les données sont en général stockées dans les mêmes tables. Il est alors possible d'effectuer les mêmes demandes de données sur différentes entreprises utilisant le même PGI. Ces tests permettent de s'assurer que les principaux processus sont correctement contrôlés. Les processus spécifiques à chaque entreprise feront l'objet d'une étude et d'une adaptation particulière.

2.7. Récurrence / fréquence des tests

Il est utile dans le cas de tests récurrents d'un exercice à l'autre, tels que la confirmation directe des clients ou le calcul des indemnités de départ à la retraite, de prévoir une procédure automatique de tests. Dans ce cas, il convient de s'assurer de la reprise des fichiers et des programmes d'une année à l'autre, en utilisant un outil adapté.

3. IDENTIFICATION DES RESSOURCES NECESSAIRES A LA MISE EN ŒUVRE DES TECHNIQUES D'AUDIT ASSISTEES PAR ORDINATEUR

3.1. Réflexions préalables à la mise en œuvre des techniques d'audit assistées par ordinateur

La décision de mettre en œuvre des techniques d'audit assistées par ordinateur, dans le cadre de la mission d'audit, implique les choix suivants :

- faut-il se doter de compétences en interne ou faut-il faire appel à des experts extérieurs ?
- quel est l'effectif requis et comment intégrer les techniques d'audit assistées par ordinateur dans la réalisation des procédures d'audit ?
- la capacité des ordinateurs dont dispose le cabinet est-elle suffisante ou faut-il investir dans un matériel plus puissant ?

- quels sont les logiciels informatiques requis pour ce type de travaux et lequel choisir ?
- quel est le coût engendré par la mise en place de cette technique et quel retour sur investissement peut-on en espérer ?
- quels sont les critères de réussite de la mise en place d'une telle technique ?

La réponse à ces questions implique une réflexion préliminaire sur l'objectif des techniques assistées par ordinateur, c'est-à-dire leur rôle au sein de l'activité de commissariat aux comptes. Les principaux facteurs à considérer sont le type de clientèle, la complexité des activités du client et la stratégie du cabinet.

Le type de clientèle a une influence dans le choix des moyens humains et matériels mis en oeuvre. Dans le cas d'une clientèle majoritairement composée d'entreprises ayant un nombre de transactions commerciales conséquent (achats, ventes, téléphonie, courtiers d'assurance, banques, etc.), la mission ne peut plus être menée sans prendre en compte les systèmes d'information et fait nécessairement intervenir des outils informatiques. Ces contraintes pèsent sur le cabinet qui devra être doté de moyens suffisants pour répondre à des demandes de travaux beaucoup plus complexes que s'il s'agissait d'un client de moindre taille.

Ceci est d'autant plus vrai lorsque certains processus font l'objet de complexités particulières (tarification avec plusieurs niveaux de remise, processus de provisionnement des stocks s'appuyant sur plusieurs critères, etc.). L'utilisation d'un logiciel de traitement des données est alors appropriée. Les fonctionnalités en standard de ce type de logiciel facilitent les rapprochements, les exécutent plus rapidement et limitent les risques d'erreur. De plus, la capacité de traitement de ces logiciels est quasi illimitée.

La stratégie du cabinet est un autre critère déterminant les moyens à mettre en œuvre. Selon les moyens qui lui sont alloués et la confiance témoignée dans la mise en place des techniques d'audit assistées par ordinateur, il pourra être envisagé de créer une véritable cellule d'expertise grâce au recrutement d'une personne expérimentée et à l'acquisition de matériels adéquats. Cette approche est recommandée si l'on envisage de recourir aux techniques d'audit assistées par ordinateur sur toutes les missions.

L'étude de ces facteurs permet de retenir l'une des deux stratégies suivantes :

- stratégie « ambitieuse » pour les structures étant prêtes à s'investir dans cette activité et à développer une véritable expertise en analyse de données,
- stratégie « prudente » pour les structures souhaitant faire de l'analyse de données tout en limitant les investissements.

3.2. Stratégie « ambitieuse »

Si le cabinet souhaite développer une expertise en analyse de données, il doit se doter de moyens appropriés, en considérant le coût et le retour sur investissement.

3.2.1. Outil

Comme cela a été présenté précédemment, la mise en place des techniques d'audit assistées par ordinateur, le contexte et la nature des missions concernées, posent un certain nombre d'exigences au niveau informatique. En effet, il faut pouvoir compter sur une capacité de traitement importante, des fonctionnalités facilitant les traitements, la possibilité d'automatiser certaines tâches, etc. En

considérant ces contraintes, l'utilisation d'un logiciel dédié au traitement des données peut permettre un meilleur audit en rationalisation les tests.

Les logiciels de traitement des données disposent de fonctionnalités particulièrement adaptées à cette activité, notamment :

- la traçabilité : le système garde en mémoire toutes les opérations effectuées sur le fichier, permettant d'expliquer la méthode de traitement et de disposer d'une piste d'audit,
- l'intangibilité des données : une fois intégrées dans le logiciel, les données ne peuvent absolument pas être modifiées,
- la reprise et la conversion des données : possibilité de traiter un grand nombre de formats de données,
- la facilité d'utilisation : le travail sur les données est facilité grâce à l'existence de quelques commandes permettant d'exécuter la plupart des traitements,
- l'automatisation des travaux récurrents.

Ces logiciels permettent d'obtenir une meilleure qualité et une meilleure productivité que les outils bureautiques standards :

- l'effacement des données initiales est impossible du fait de l'intangibilité des données,
- le contrôle des travaux est effectué au moyen du système de conservation des historiques,
- la mise en place de programmes standardisés permet de gagner en productivité.

3.2.2. Profil

L'utilisation d'un logiciel de traitement des données ne peut être effectuée que par un collaborateur ayant une connaissance approfondie de l'audit financier et des compétences informatiques. Cette double compétence (par exemple, un cursus d'ingénieur complété d'une spécialisation en système d'information) est une ressource rare sur le marché du travail car très recherchée. Il existe cependant d'autres profils convenant à ce type de travaux, mais il faudra choisir entre une dominante technique ou une dominante audit.

Le recours à un technicien permet d'être opérationnel rapidement sur les aspects techniques des travaux de traitement des données. La période de formation sera davantage consacrée à acquérir les bases de l'audit financier, nécessaires pour identifier les données utiles et produire des analyses pertinentes. Il est essentiel pour la réussite de la mise en place d'une telle compétence, que les rapports produits répondent aux attentes du commissaire aux comptes.

Le recours à un auditeur financier plutôt qu'à un technicien est préférable, en raison de sa connaissance des besoins du commissaire aux comptes. Il sera mieux à même d'orienter ses travaux pour répondre aux besoins de la mission d'audit et de définir les données nécessaires pour produire des résultats pertinents. La durée d'apprentissage de l'outil et des compétences informatiques induites sera fonction des aptitudes du collaborateur. Le développement d'une expertise représente un réel investissement en temps, c'est pourquoi il convient de choisir un collaborateur particulièrement motivé. Il est particulièrement important de choisir des tests simples à réaliser lors des premières missions, puis d'augmenter la complexité au fur et à mesure de la maîtrise de l'outil. Suite à cette phase d'apprentissage, le collaborateur se focalisera davantage sur l'analyse que sur la programmation, pour réduire le risque de découragement et d'erreurs dans les traitements.

3.2.3. Matériel

Pour mener les techniques d'audit assistées par ordinateur, il est préférable de disposer d'un ordinateur de type PC, celui-ci étant le standard utilisé par les entreprises. La capacité du disque doit être suffisante pour permettre de stocker les données des clients afin de pouvoir capitaliser les travaux d'une année sur l'autre. Une capacité de 10 Go est souvent un minimum.

Un graveur de CD-ROM permet d'effectuer des sauvegardes non modifiables et de lire les données que les clients transmettent sous forme de CD-ROM. Certains clients fournissent leurs données sur d'autres supports. Il est alors nécessaire de disposer des lecteurs correspondants.

3.3. Stratégie « prudente »

Si le cabinet d'audit ne dispose pas des moyens suffisants pour investir dans du matériel spécifique et ne s'adresse qu'à des clients de taille réduite, il est possible d'utiliser un logiciel bureautique, de type tableur standard. Il peut s'agir d'une solution transitoire avant d'entreprendre des investissements plus importants.

La stratégie « prudente » présente l'avantage d'utiliser les moyens déjà existants au sein du cabinet :

- le matériel est un PC du cabinet. Le logiciel utilisé est un tableur, installé généralement en standard sur tous les postes utilisant des outils bureautiques. Son utilisation est connue des collaborateurs,
- un collaborateur expérimenté du cabinet pourra effectuer les opérations de tests avec le tableur.

Cette configuration permet de débuter des analyses de données en limitant les difficultés rencontrées au démarrage. L'investissement pour le cabinet se résume au temps consacré par le collaborateur pour se familiariser avec l'outil et avec les programmes de test.

3.4. Règles et risques communs

Dans le cas d'une stratégie « prudente » où le recrutement externe n'est pas envisagé, il est conseillé de ne former qu'une seule ressource, plutôt que de répartir cette fonction sur plusieurs collaborateurs à temps partiel, l'acquisition des compétences étant longue et devant rester concentrée. Le collaborateur ne peut pleinement s'investir dans une telle activité que s'il la pratique régulièrement.

En revanche, cette concentration du savoir représente un risque pour le cabinet en cas de départ ou d'absence prolongée de l'unique collaborateur compétent, les travaux d'analyse de données et peut-être même certaines missions ne pouvant être menées à bien du fait de l'impossibilité de le remplacer.

Les risques liés à l'analyse de données consistent à détecter de fausses anomalies ou à ne pas détecter de vraies anomalies qui, si elles avaient été détectées, auraient conduit à émettre des réserves sur les comptes. Ces risques proviennent le plus souvent de la réalisation de tests non pertinents ou d'erreurs dans la programmation des contrôles.

Lorsque les ressources en interne ne permettent pas de mener ces travaux au sein du cabinet, ou lorsque les risques de mise en œuvre et d'analyse sont jugés trop élevés, il est préférable de recourir à

un expert indépendant pour réaliser la mission et/ou pour accompagner l'auditeur dans les premières missions.

3.5. Procédures préalables

Les étapes suivantes doivent être respectées :

- s'assurer que les critères choisis seront probants par rapport à l'objectif visé par le test,
- protéger les données initiales et conserver la piste d'audit,
- mettre en forme et classer les données :
  - agréger une population selon des critères numériques ou selon la nature commune des éléments. Cette opération s'avère particulièrement utile pour obtenir par exemple une reconstitution de la balance auxiliaire clients à partir du détail des écritures, ou encore pour obtenir le total des ventes par produit en volume et en montant à partir du détail du fichier des ventes,
  - trier une population selon les critères identifiés,
  - créer un fichier à partir d'un autre en reprenant certains enregistrements et certains champs clés,
  - mettre plusieurs fichiers les uns à la suite des autres dans un nouveau fichier,
- analyser les résultats :
  - disposer de statistiques sur une valeur (moyenne, somme et nombre de valeurs positives et négatives, dispersion, etc.),
  - insérer un champ calculé dans le fichier,
  - sélectionner statistiquement des données dans le fichier,
  - rapprocher deux fichiers disposant d'une même clé. Par exemple, rapprocher le fichier des factures clients du fichier des adresses clients, pour disposer de toutes les informations nécessaires à la confirmation directe des factures (montant des factures et adresses),
- présenter les résultats :
  - éditer les résultats,
  - exporter les champs utiles dans un nouveau fichier.

Le tableau ci-dessous présente une correspondance entre les objectifs du commissaire aux comptes et la traduction en termes de techniques d'audit assistées par ordinateur.

Besoins du commissaire aux comptes	Intervention sur les données
• Analyser les stocks en fonction du dépôt, de la zone géographique, de la famille d'articles, etc. • Répartir les stocks en valeur (faible, moyenne, importante)	Agréger une population selon des critères numériques ou selon la nature commune des éléments
Rechercher : • Les stocks négatifs • Les prix à valeur nulle • Les montants les plus importants • Les clients créditeurs	Exporter les champs utiles dans un nouveau fichier
• Trier un fichier pour en faciliter la lisibilité ultérieure • Sélectionner les valeurs les plus importantes (factures, ventes, achats, clients)	Trier une population selon des critères numériques ou selon la nature commune des éléments
• Rechercher les doublons (facture, salaire double, double facture fournisseur) • Créer des fichiers cumulés (par exemple : balance clients à partir d'un grand livre auxiliaire client)	Agréger une population selon des critères numériques ou selon la nature commune des éléments pour création d'un fichier exploitable
Exploiter les données sous un autre logiciel	Exporter certains champs du fichier dans un nouveau fichier de format différent et exploitable sur un autre logiciel
Rassembler dans un seul fichier les informations qu'un client fournit dans plusieurs fichiers	Mettre plusieurs fichiers les uns à la suite des autres dans un nouveau fichier
Disposer de statistiques (moyenne, somme et nombre de valeurs positives et négatives, valeurs extrêmes, etc.)	Calculer la moyenne, minimum, maximum et les valeurs extrêmes
Mise en place d'algorithmes (valorisation et dépréciation des stocks, dépréciation des stocks, comptes clients, dotations aux amortissements, etc.)	Insérer un champ calculé dans le fichier
Confirmation clients et fournisseurs Inventaire statistique (stocks, immobilisations)	Sélectionner statistiquement des données dans le fichier
• Comparer des fichiers pour détecter les anomalies (expédition sans vente, réception sans achat) • Rassembler dans un seul fichier les informations issues de deux autres fichiers : valorisation des stocks avec quantités dans l'un et prix de revient dans l'autre	Rapprocher deux fichiers disposant d'une même clé

3.6. Sélection du logiciel de traitement

La sélection du logiciel de traitement, outil dédié ou outil standard comme un tableur par exemple, est fonction :

- des caractéristiques du cabinet et des entreprises clientes,
- des opérations à effectuer sur les données,
- des fonctionnalités offertes par l'outil.

Les principales fonctionnalités à prendre en compte dans le processus de sélection sont les suivantes :

- sécurité de la reprise : peut-on sécuriser le contenu des fichiers initiaux ?
- programmation : peut-on utiliser et stocker une série de requêtes ?
- taille des fichiers : existe-t-il une limite en taille des fichiers traités ?
- conservation des modèles de requête ou de travail : peut-on réutiliser les mêmes requêtes d'un client à un autre ?
- données de contrôle : peut-on contrôler l'exécution des requêtes grâce à un compte-rendu d'exécution ?
- indexation : peut-on utiliser et stocker des index pour trier les fichiers de taille importante ?
- tableaux de bord : existe-t-il des fonctions pour éditer les résultats sous une forme synthétique (graphique, tableaux, etc.) ?
- modèles d'analyse : existe-t-il des modèles préconçus par type d'analyse ?

Cette description des fonctionnalités n'est pas exhaustive, mais elle permet d'appréhender :

- les possibilités offertes par chaque outil,
- l'adéquation de ces fonctionnalités avec l'audit financier,
- le degré de technicité exigé afin de pouvoir les exploiter efficacement.

4. ETAPES DE LA MISE EN ŒUVRE DES TECHNIQUES D'AUDIT ASSISTEES PAR ORDINATEUR

4.1. Récupération des fichiers informatiques

Il convient de définir avec l'entreprise la nature des tests à réaliser sur la base d'un cahier des charges. L'objectif est de réunir les compétences informatiques et comptables des auditeurs avec la connaissance métier du client pour :

- identifier les risques,
- définir les données nécessaires à exploiter,
- récupérer les fichiers nécessaires à la réalisation des tests informatiques utiles à l'audit, sur bande magnétique, sur cartouche ou CD-ROM.

Une première difficulté apparaît du fait de l'existence dans les entreprises de systèmes diversifiés et de progiciels d'origine différente, qui ne gèrent pas le même type de données. La récupération des fichiers à un format et sur un support adaptés est une phase essentielle mais complexe, compte tenu de la diversité des systèmes informatiques dans les entreprises (logiciels spécifiques, progiciels, différences de technologie…). Le format des supports de données reçus est très varié. A titre d'exemple, on peu citer :

- les disquettes 3 pouces 1/2 (pour les fichiers de faible taille),
- les bandes magnétiques 1600 BPI qui peuvent contenir près de 40 Mo de données,
- les cartouches 3480 qui peuvent contenir plus de 200 Mo,
- les cartouches DAT 4 mm et 8 mm qui peuvent contenir respectivement 5 et 7 Go.

Dans les petites et moyennes entreprises, la récupération des données concerne généralement un volume inférieur à un giga octets.

4.2. Validation des fichiers

Elle s'effectue notamment par rapprochement des fichiers reçus avec la comptabilité. Il s'agit de vérifier, avant d'effectuer les tests, que les données reçues sont exhaustives et qu'elles n'ont subi aucune modification lors de l'extraction.

4.3. Réalisation des tests

Le passage à la phase de codage, le contrôle des programmes réalisés et le lancement des tests peuvent alors démarrer. Cette phase ne constitue généralement pas une difficulté majeure ; elle présente toutefois une particularité technique liée au logiciel de traitement sélectionné. Il est important que les tests réalisés soient reproduits ultérieurement et que toutes les étapes intermédiaires soient sauvegardées. Ainsi, l'existence d'un journal des tests effectués dans le logiciel d'audit sélectionné peut s'avérer utile pour leur identification. Cette phase aboutit à la constitution d'un dossier contenant les différentes étapes du cycle de réalisation et de validation.

4.4. Analyse et synthèse

La dernière phase consiste à analyser et à interpréter les résultats, qui sont alors consignés dans un rapport de synthèse décrivant notamment les tests réalisés et les recommandations qui en découlent.

5. EXEMPLES DE MISE EN ŒUVRE DE TECHNIQUES D'AUDIT ASSISTEES PAR ORDINATEUR

5.1. Exemples de base

5.1.1. Cycle Achats : exemple 1

A. Objectif

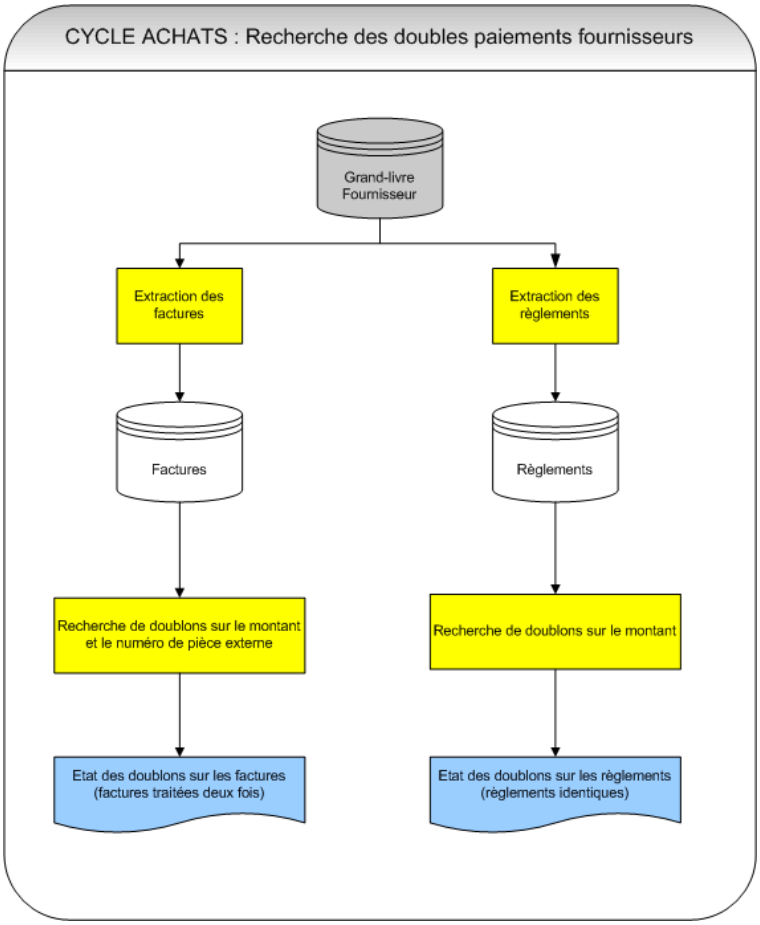
Rechercher les fournisseurs qui ont été payés deux fois.

B. Test

Deux tests informatiques peuvent être effectués :

- les doubles enregistrements de facture,
- les doubles règlements.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Extraction des factures et des règlements	Extraction
Recherche de doublon sur le montant et le numéro de pièce	Agréger la population sur le montant et le numéro de pièce

D. Recommandations

- Disposer d'un numéro de pièce du fournisseur pour effectuer les recherches de doublons, le montant ne s'avérant pas toujours suffisant pour ne détecter que les vraies anomalies.
- Travailler sur des comptabilités dans lesquelles les factures sont réglées séparément et dont les montants des règlements sont différents.

Cette procédure s'avère inefficace en cas de règlements groupés. Il convient alors d'effectuer des contrôles substantifs étendus.

5.1.2. Cycle Achats : exemple 2

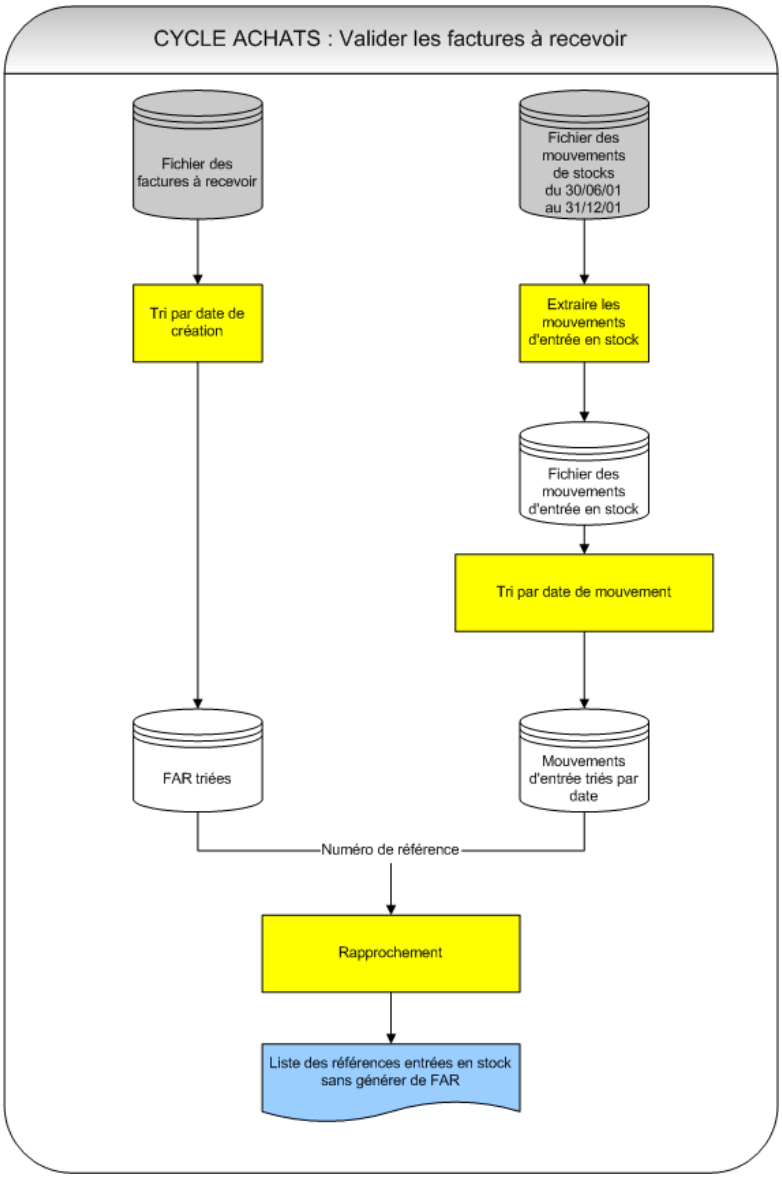
A. Objectif

Valider les factures à recevoir.

B. Tests

Les progiciels détectent et évaluent les factures à recevoir à partir des bons de réceptions non facturés. A partir du fichier des mouvements de stocks, il est possible de contrôler les quantités reçues et vérifier la valorisation.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Comparaison de fichiers pour détecter les anomalies (références entrées en stock sans générer de factures à recevoir)	Rapprocher deux fichiers disposant d'une même clé (le numéro de référence par exemple)

D. Anomalie possible

Suite à des problèmes d'exploitation informatique, les factures à recevoir ne sont pas créées pour certains types d'entrées.

E. Recommandations

- Identifier les mouvements de stocks à prendre en compte.
- Comprendre le fonctionnement des différents lieux de stockage (prise en compte ou non des stocks en contrôle qualité) et des règles de propriétés (franco, sortie usine, etc.).

5.1.3. Cycle Stocks

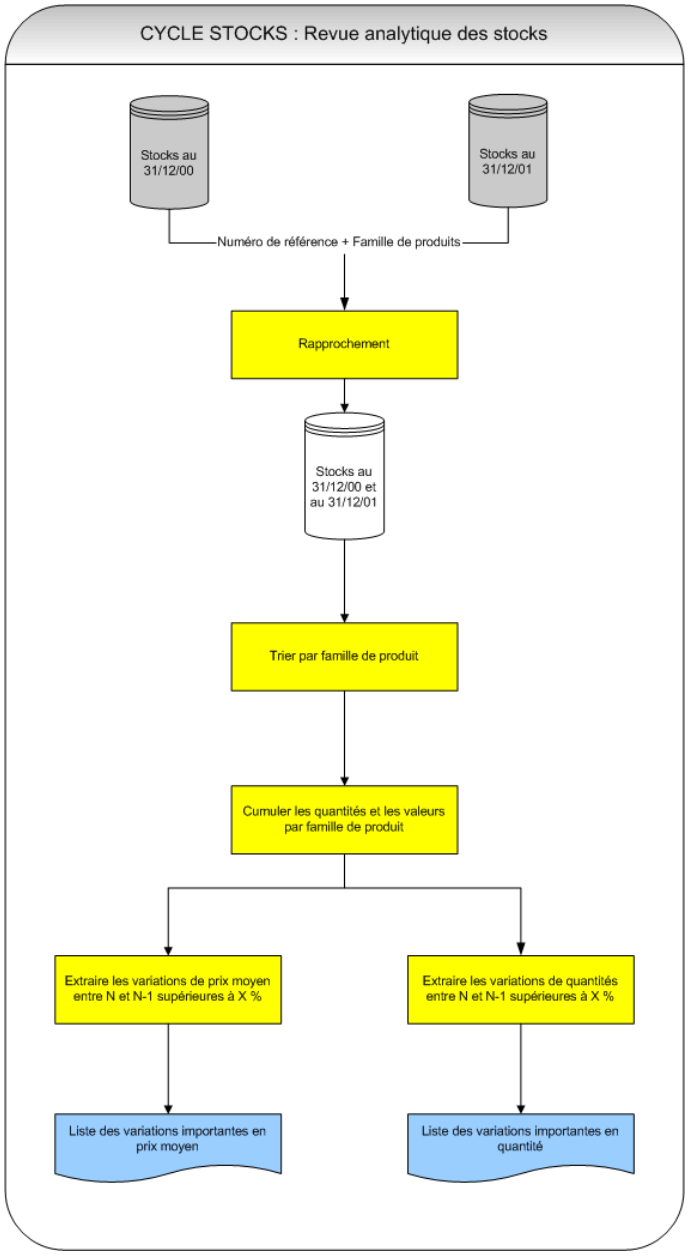
A. Objectif

Réaliser un examen analytique des stocks.

B. Test

A partir des états de stocks, effectuer des rapprochements par rapport aux inventaires antérieurs.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Rassembler dans un seul fichier les informations issues de deux autres fichiers (en l'espèce, la valorisation des stocks sur deux années consécutives)	Rapprocher les deux fichiers disposant d'une même clé
Trier le fichier pour faciliter la lisibilité ultérieure	Tri
Créer un fichier cumulé (par exemple par famille d'articles)	Cumul
Identifier : ▪ Les variations significatives de prix moyen ▪ Les variations significatives de quantité	Extraction

D. Anomalies possibles

Cet examen analytique des stocks permet de détecter :

- des variations anormales de certaines catégories de stocks et peut révéler par exemples, des stocks absents, des oublis de comptage, des stocks comptés en double, des erreurs sur le prix de revient (dues à des erreurs sur la prise en compte des remises ou à des erreurs dans les unités de valorisation),
- des problèmes liés à l'activité ou d'identifier des opérations spéculatives liées aux matières premières (achat de plastique en grande quantité avant une montée des prix du pétrole).

E. Recommandations

- Disposer d'un fichier permettant une analyse par famille, soit dans un champ spécifique, soit par l'analyse des caractères de la référence.
- Disposer d'inventaires fréquents pour effectuer des analyses sur des périodes inférieures à un an.

5.1.4. Cycle Ventes : exemple 1

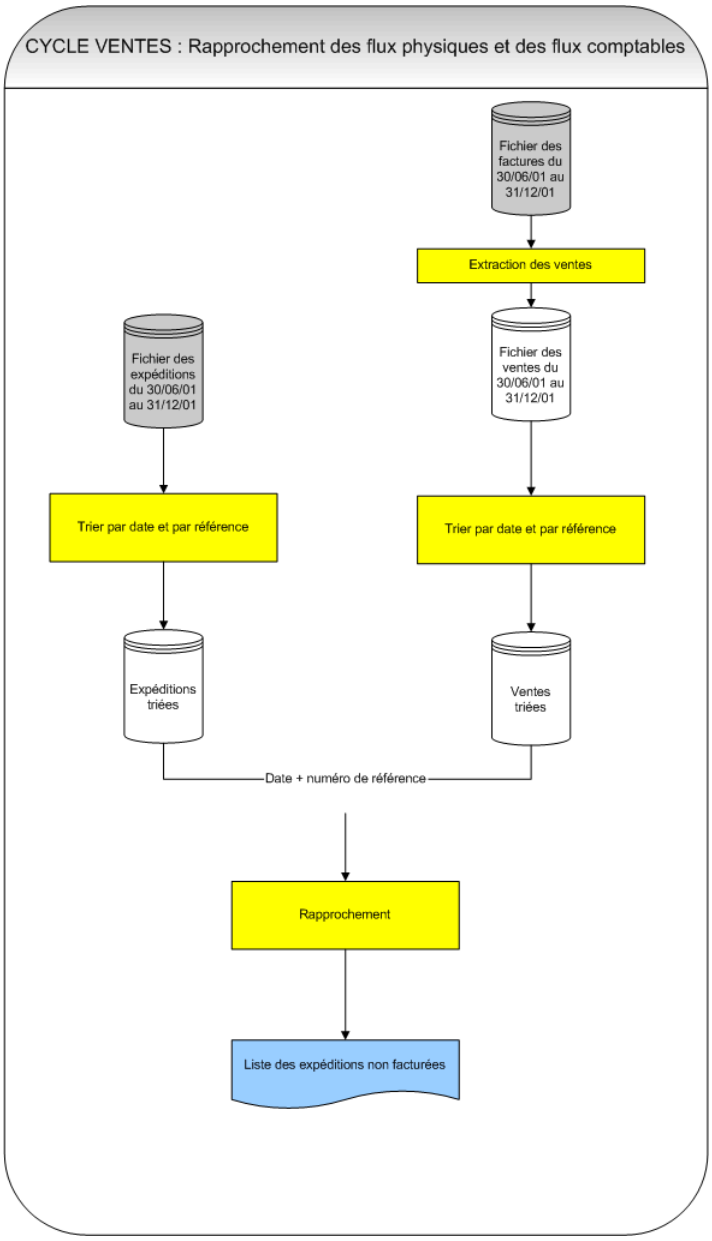
A. Objectif

Rapprocher les flux physiques et les flux comptables.

B. Test

A partir du fichier des mouvements de stocks et du fichier de facturation, identifier les expéditions qui n'ont pas été facturées.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Rechercher les ventes	Extraction
Trier un fichier pour faciliter la lisibilité ultérieure	Tri
Comparaison de fichiers pour détecter les anomalies (expédition sans facture)	Rapprochement

D. Anomalie possible

Suite à des faiblesses de la procédure liée à la facturation, des livraisons « clients » peuvent ne pas être facturées.

E. Recommandations

- Identifier la périodicité de facturation par rapport aux mouvements de stocks.
- Disposer d'un fichier complet de la facturation dont les éléments peuvent être rapprochés avec ceux du fichier des mouvements de stocks.

5.1.5. Cycle Ventes : exemple 2

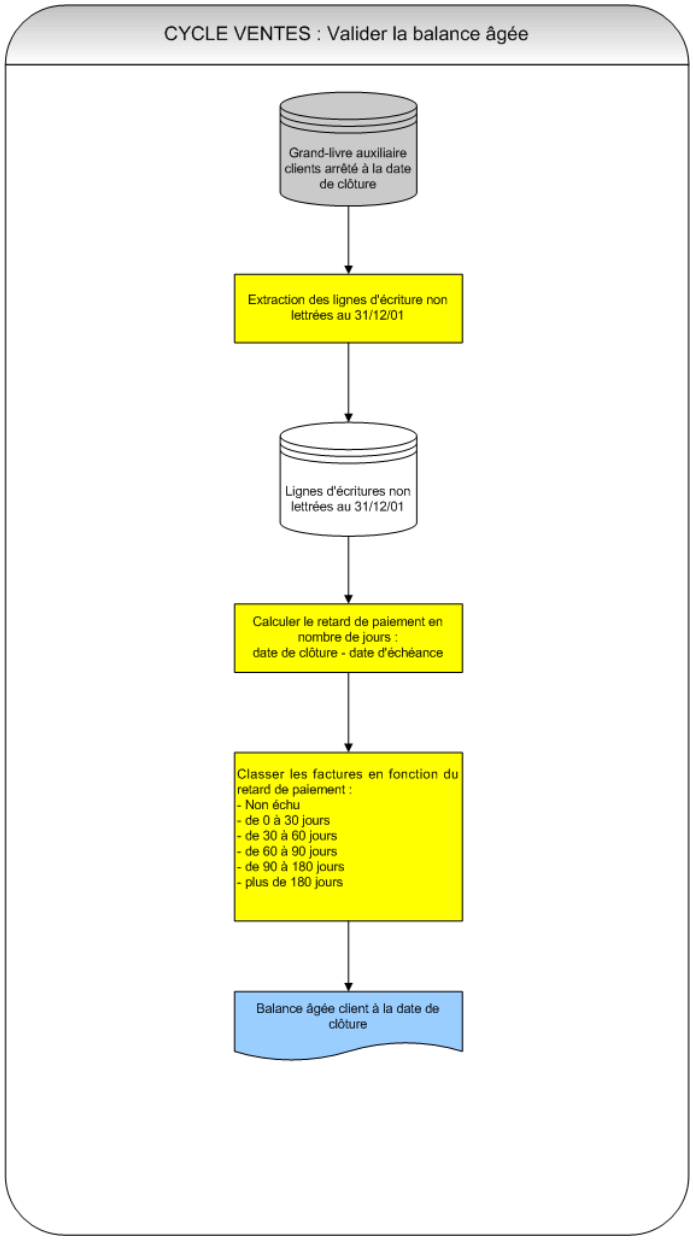
A. Objectif

Valider la balance âgée.

B. Test

A partir du fichier « grand-livre auxiliaire des clients », reconstituer une balance âgée à date afin de valider la balance âgée fournie par le client.

C. Réalisation du test



Procédures à mettre en œuvre :

Besoin	***Intervention sur les données***
Rechercher les écritures non lettrées	Extraction
Mise en place d'algorithmes : calcul du retard de paiement	Insertion d'un champ calculé dans le fichier
Classer les écritures non lettrées en fonction du retard de paiement	Agrégation de la population selon le retard de paiement

D. Anomalie possible

Certains systèmes informatiques ne prévoient pas l'édition de balances par antériorité des créances, ce qui rend difficile la réalisation de ce test important.

E. Recommandation

Pour obtenir un fichier contenant uniquement les écritures non lettrées à la date de clôture, utiliser de préférence les dates de lettrage des opérations, ou à défaut, extraire les données à la date de clôture.

5.1.6. Cycle Immobilisations : exemple 1

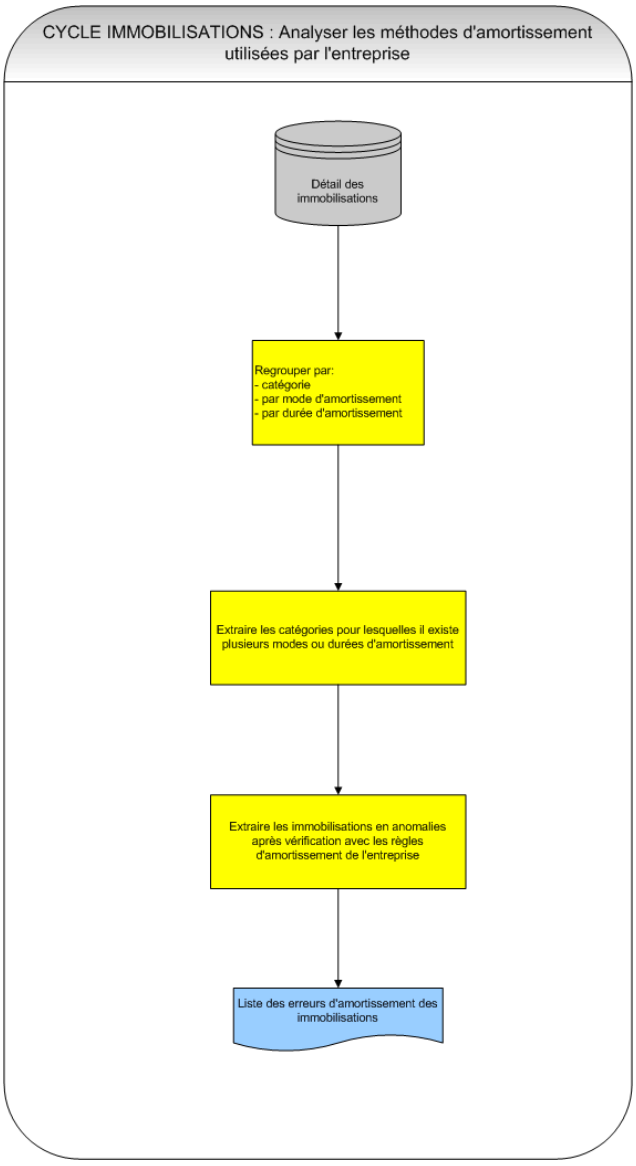
A. Objectif

Analyser les méthodes d'amortissement utilisées par l'entreprise.

B. Test

A partir du fichier des immobilisations, regrouper les immobilisations par nature, par méthode et par durée d'amortissement.

C. Réalisation



Procédures à mettre en œuvre :

Besoin	***Intervention sur les données***
Analyser les immobilisations par nature suivant la durée d'amortissement	Agrégation de la population selon la durée d'amortissement
Rechercher les catégories pour lesquelles il existe plusieurs méthodes d'amortissement	Extraction
Rechercher les anomalies dans le calcul des amortissements	Extraction

D. Anomalie possible

Cette analyse permet de vérifier l'homogénéité des méthodes d'amortissement utilisées par l'entreprise. En effet, des immobilisations de même nature peuvent avoir des méthodes et des durées d'amortissement différentes si une procédure n'est pas mise en place et testée régulièrement.
Ce contrôle peut être effectué sur plusieurs années afin de vérifier la permanence des méthodes d'évaluation comptable et la continuité des plans d'amortissement. Il permet également de détecter les erreurs de classement des immobilisations et les erreurs de saisie des méthodes d'amortissement.

E. Recommandations

- Disposer d'une segmentation par famille au sein d'un même compte pour identifier les immobilisations devant être amorties différemment.
- Effectuer ce test d'une année sur l'autre pour permettre une validation exhaustive à chaque clôture.

5.1.7. Cycle immobilisations : exemple 2

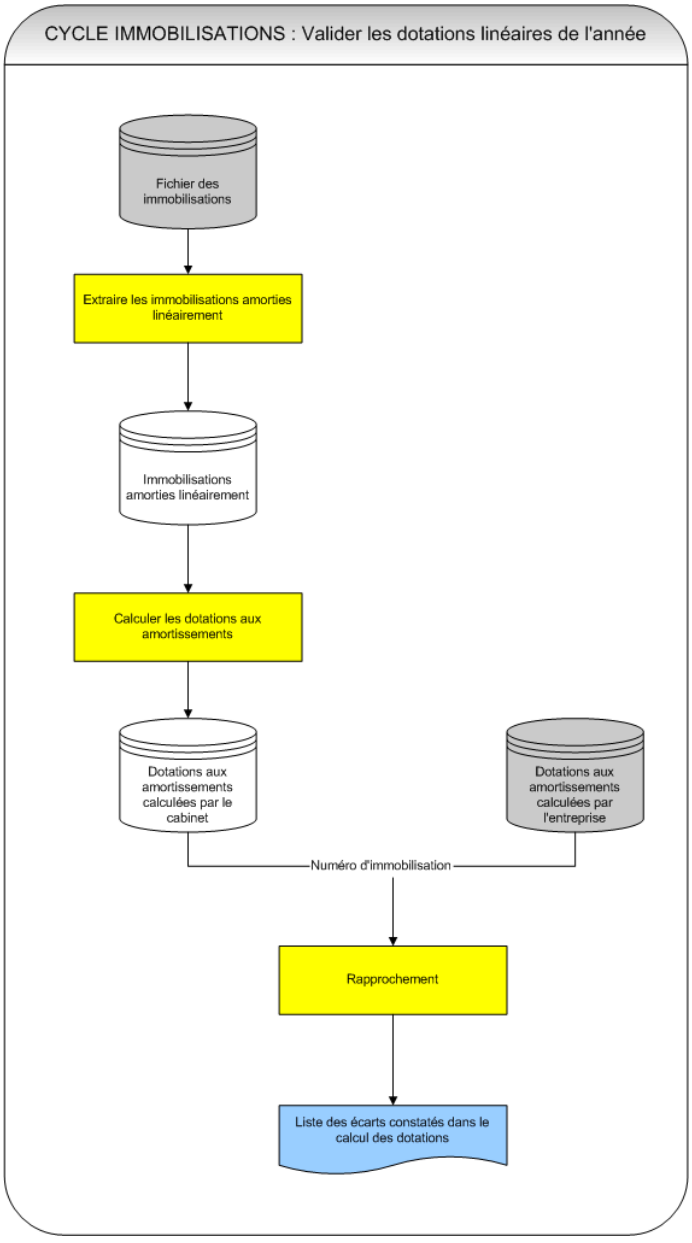
A. Objectif

Valider les dotations aux amortissements linéaires de l'année.

B. Test

A partir d'un fichier d'amortissement des immobilisations, valider la dotation aux amortissements linéaires calculée par l'entreprise.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Rechercher les immobilisations amorties linéairement	Extraction
Calculer les dotations aux amortissements	Insérer un champ calculé dans le fichier

D. Anomalie possible :

Suite à des erreurs dans l'utilisation du logiciel par l'entreprise, des immobilisations mises en service ne sont pas amorties. Des anomalies sont générées lorsque la valeur d'acquisition de l'immobilisation est modifiée après sa mise en service.

E. Recommandations

- Créer un programme standard, pour le calcul de l'amortissement linéaire et pour le calcul de l'amortissement dégressif, qui peut être utilisé pour plusieurs clients.
- Demander en priorité à l'entreprise des fichiers à plat et utiliser des fichiers d'impression dans les autres cas (états de gestion utilisés par le service comptable pour travailler sur les amortissements). Les fichiers d'impression sont utilisés en dernier recours lorsque des fichiers à plat ne sont pas disponibles.

5.1.8. Cycle Paie : exemple 1

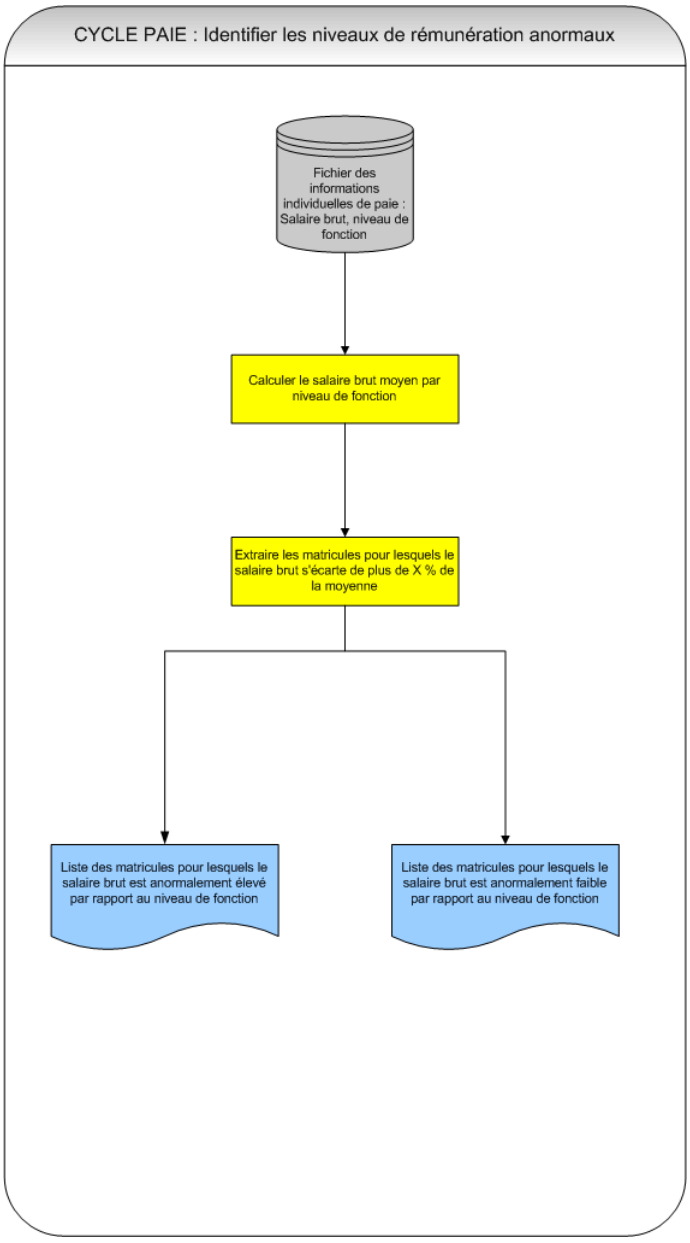
A. Objectif

Identifier les niveaux de rémunération anormaux.

B. Test

A partir des fichiers de paie, comparer les salaires des collaborateurs exerçant des fonctions identiques.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Calculer le salaire brut moyen par niveau de fonction	Insérer un champ calculé dans le fichier
Extraire les numéros matricule des salariés qui présentent un niveau de salaire anormal	Extraction

D. Anomalie possible

Le risque de disparité des salaires pour des fonctions identiques existe lorsque l'entreprise possède différents sites d'exploitation et qu'il n'y a pas de coordination entre les responsables du personnel.

E. Recommandation

Effectuer le contrôle régulièrement et vérifier la correction des anomalies.

5.1.9. Cycle Paie : exemple 2

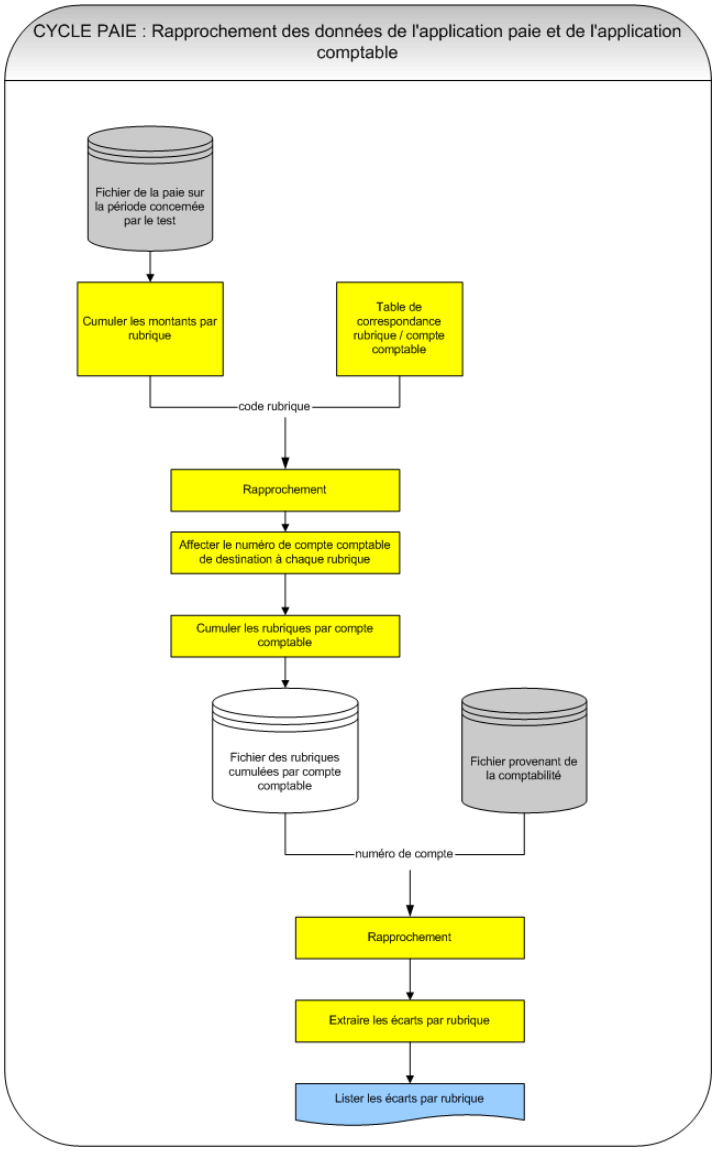
A. Objectif

Effectuer un rapprochement entre les données de l'application paie et celles de l'application comptable.

B. Test

A partir des données de calcul de la paie et des fichiers des écritures comptables, effectuer un rapprochement entre les montants calculés par l'application « Paie » et les montants comptabilisés par l'application comptable.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Cumuler les montants par rubrique	Cumul
Affecter un compte comptable à chaque rubrique de la paie	Rapprochement de fichiers
Cumuler les rubriques par compte comptable	Cumul

D. Anomalie possible

Certaines rubriques de la paie peuvent se déverser dans des comptes inappropriés en cas d'erreurs de paramétrage.

E. Recommandations

- Disposer d'une information complète sur le paramétrage des rubriques de paie en comptabilité.
- Effectuer des rapprochements sur les rubriques les plus significatives.

5.1.10. Etablissements de crédit : exemple 1

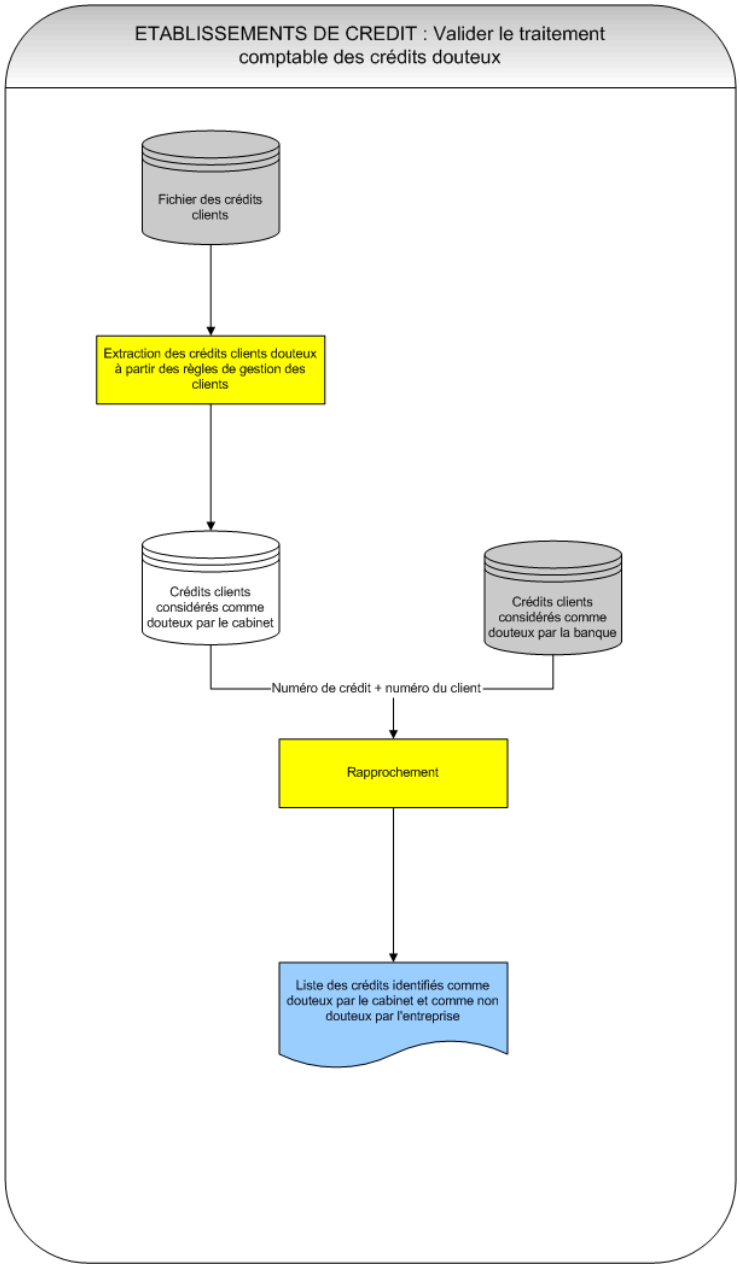
A. Objectif

Valider le traitement comptable des créances douteuses. Ce test peut également s'appliquer aux entreprises qui utilisent des critères stricts de classification des créances.

B. Test

A partir des fichiers des en-cours de crédit et des règles de gestion des clients douteux, déterminer les en-cours clients qui devraient être comptabilisés en créances douteuses.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Extraction des en-cours de crédits douteux	Extraction
Comparaison des en-cours théoriques et des en-cours présentés par l'entreprise	Rapprochement de fichiers

D. Recommandation

Connaître les règles appliquées par l'entreprise pour le traitement comptable des en-cours de crédits douteux.

5.1.11. Etablissements de crédit : exemple 2

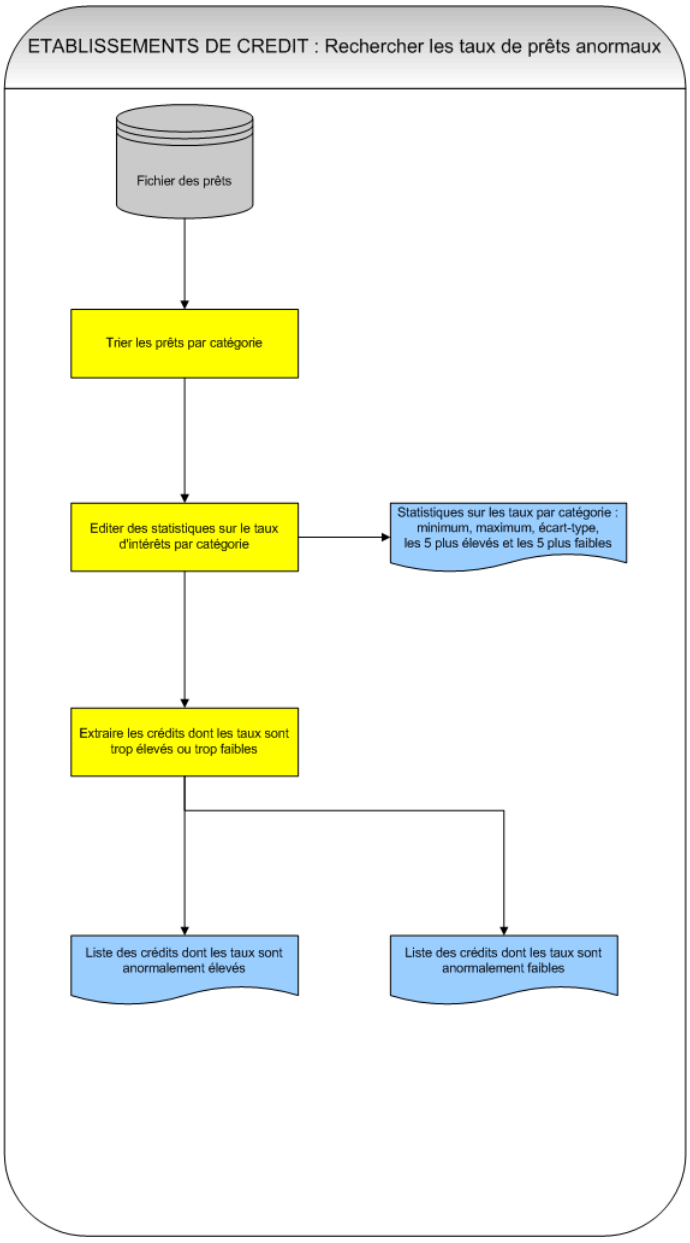
A. Objectif

Rechercher des taux de prêts anormaux.

B. Test

A partir des fichiers des en-cours de crédit par catégorie, rechercher les crédits présentant des taux anormaux.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Trier les prêts par catégorie	Tri
Editer les statistiques portant sur les taux d'intérêts	Statistiques
Extraire les crédits présentant des taux anormaux	Extraction

D. Recommandations

Il faut vérifier que les taux pratiqués effectivement ne dépassent pas le taux de l'usure.

5.1.12. Secteur des « Assurances »

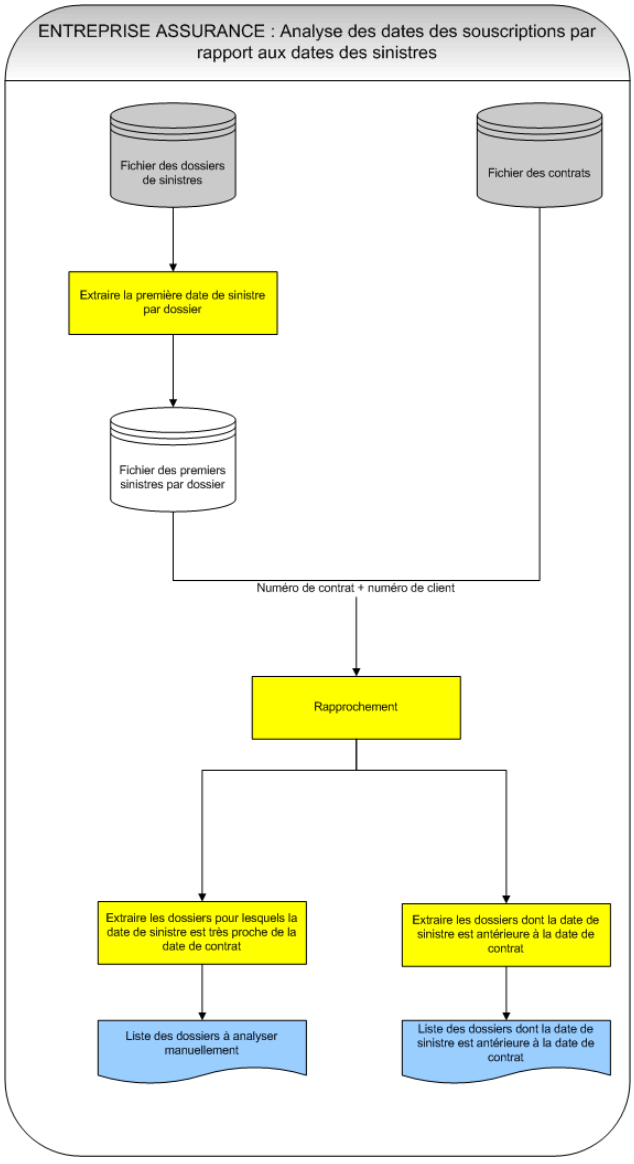
A. Objectif

Analyse des dates de souscription par rapport aux dates de sinistre. Cette analyse permet d'identifier une fraude ; l'agent ou le courtier ne déclare le contrat à la compagnie d'assurance qu'à la date du premier sinistre en conservant les primes antérieures.

B. Test

A partir du fichier des dossiers de sinistre et du fichier des contrats, rapprocher les dates de sinistre et les dates de souscription.

C. Réalisation



Procédures à mettre en oeuvre :

Besoin	***Intervention sur les données***
Dans le fichier client, extraire la date du premier sinistre	Extraction
Comparer la date de sinistre avec la date de contrat	Rapprochement de fichiers
Extraire les dossiers pour lesquels les dates de sinistres sont antérieures aux dates de contrat	Extraction

D. Recommandations

- Analyser les sinistres en effectuant des regroupements par zone géographique ou par responsable de commercialisation.
- Effectuer des contrôles sur les pièces des dossiers de sinistre.

5.2. Exemples de recherches plus élaborées

5.2.1. Cycle des achats

Contrôles possibles :

- contrôler l'interface entre l'application achats et l'application comptable,
- effectuer une confirmation directe des comptes fournisseurs,
- rechercher des factures fournisseurs sans livraison.

5.2.2. Cycle des stocks

Contrôles possibles :

- contrôler la provision pour dépréciation,
- stratifier la population,
- contrôler la valorisation.

EXEMPLE DE PROGRAMME : TESTS INFORMATIQUES SUR LES CYCLES STOCKS / FACTURATION

A. Présentation

L'objectif de ces tests est de contrôler la fiabilité des informations de la chaîne stocks/facturation.

B. Fichiers nécessaires

La mise en oeuvre des contrôles sur les stocks nécessite d'identifier préalablement les informations disponibles dans les fichiers suivants :

- fichiers des stocks sur une période de deux mois (la période peut être adaptée en fonction des besoins),
- fichier des prix unitaires,
- fichier des mouvements de stocks gérés par la chaîne commerciale pendant la période examinée,
- fichier des facturations émises au cours de cette période.

C. Méthode

1) Rapprochement entre les lignes de facturation et les en-têtes de facture

On distingue deux fichiers dans la facturation :

- le fichier des lignes de facturation qui donne des informations sur l'article facturé (qualité, quantité, etc.),
- le fichier des en-têtes de facture qui reprend ces informations et indique également les conditions accordées au client (taux de remise, etc.).

Il est indispensable d'effectuer ce rapprochement car seules les en-têtes de facture reprennent l'ensemble des données de valorisation des factures et pourront donc, à ce titre, être comparées à la comptabilité.

2) Rapprochement des fichiers de stock commercial avec le stock apparaissant en comptabilité

Il est nécessaire de s'assurer de la correspondance de ces fichiers de stocks à chaque arrêté comptable.

3) Validation du fichier des mouvements de stocks

La facturation est générée par les informations contenues dans le fichier des mouvements de stocks. Il convient de valider ces informations par un test consistant à reconstituer les stocks d'une date à une autre en fonction des mouvements de la période considérée (Stock M = Stock M-1 + Mouvements de la période). Ce test permet alors de s'assurer que le fichier des mouvements reprend bien tous les mouvements de stocks de la période concernée et seulement ceux-ci.

4) Rapprochement entre le fichier des mouvements de stocks et les lignes de facturation

Ce rapprochement a pour objectifs :

- de rechercher les sorties de stocks identifiés comme facturables dans la chaîne commerciale n'ayant pas donné lieu à facturation,
- de rechercher les facturations émises alors qu'aucune sortie n'a été identifiée dans le fichier des mouvements,
- d'identifier les écarts entre les quantités sorties et les quantités facturées.

5.2.3. Cycle des ventes

Contrôles possibles :

- contrôler l'interface entre l'application ventes et l'application comptable,
- effectuer une confirmation directe des clients,
- identifier les facturations émises sans émission de bons de livraison,
- identifier les factures à établir.

EXEMPLE DE PROGRAMME : CONFIRMATION DIRECTE DES FACTURATIONS AUX CLIENTS

A. Présentation

Cette confirmation directe consiste à sélectionner par sondage des factures parmi l'ensemble des factures non réglées à la date de l'arrêté et à demander aux clients correspondants de confirmer leur réalité. Le test est à utiliser uniquement lorsque les comptes clients comportent de nombreuses écritures ou lorsque les clients circularisés n'ont pas les systèmes comptables permettant de répondre sur les soldes. La confirmation doit intervenir pendant l'exercice et non à la date de clôture. Il s'agit plus d'un test portant sur les systèmes que sur les actifs.

B. Fichiers nécessaires

Il est nécessaire d'obtenir les éléments suivants :
- le grand-livre auxiliaire des clients à la date d'arrêté comptable,
- le fichier des adresses des clients.

C. Méthode retenue

1) Rapprochement de l'extraction avec la base comptable

2) Elaboration d'une balance par antériorité des soldes

3) Détermination de la taille de l'échantillon

4) Sélection et édition des lettres de confirmation sur papier à en-tête de la société

D. Réalisation des tests

1) Elaboration d'une balance par antériorité des soldes

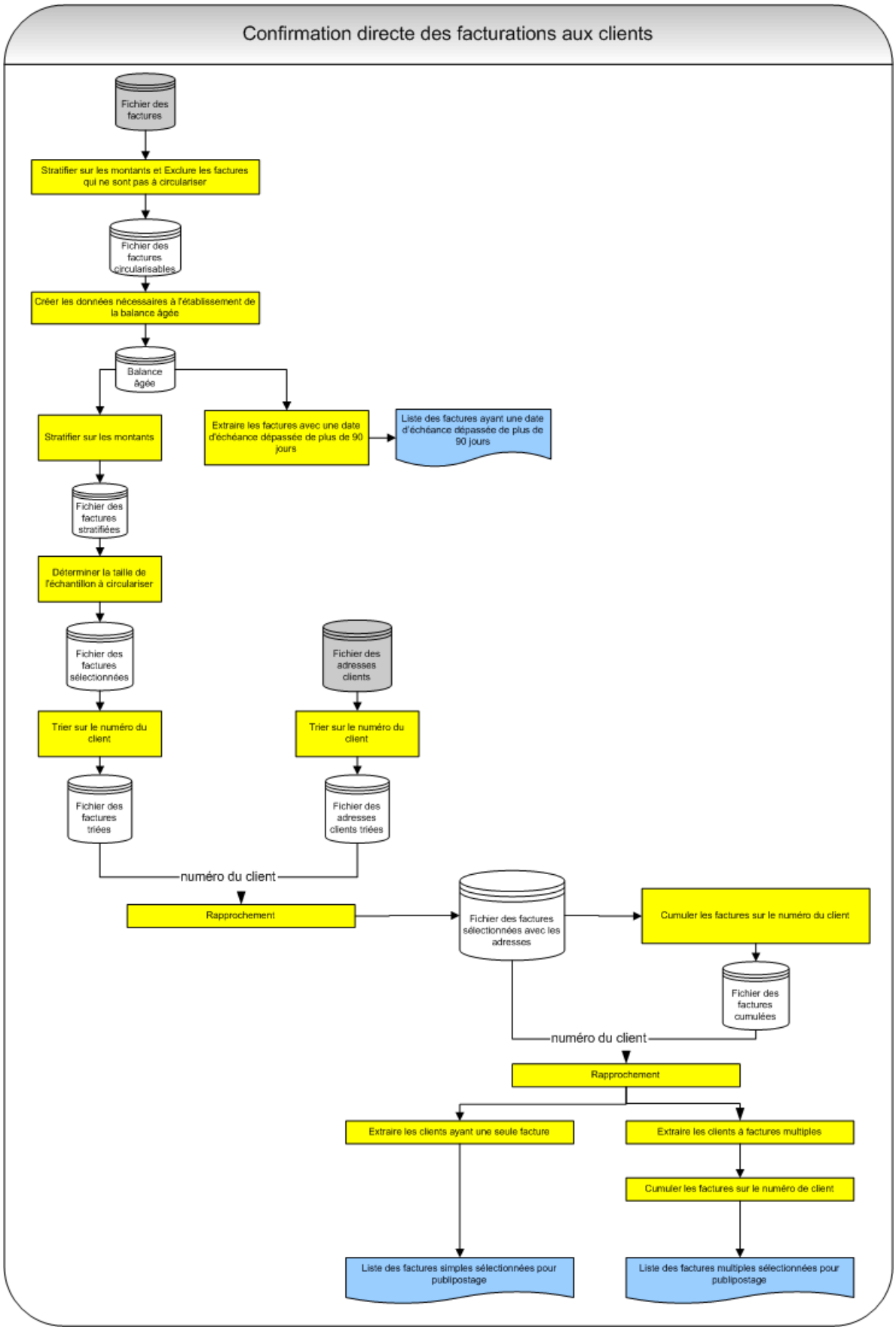
A partir de la date d'échéance et du montant signé de chaque facture ou avoir, classer chaque pièce en fonction du nombre de jours entre la date de clôture et la date d'échéance.

2) Détermination de la taille de l'échantillon

Il convient de déterminer la population devant faire l'objet d'une confirmation. A partir du grand-livre auxiliaire clients des écritures non lettrées, retirer les éléments du type avoirs, opérations diverses, pour n'avoir que les numéros de factures, numéros de clients et montants.
Ensuite, en vue de déterminer statistiquement la taille de l'échantillon, il convient de stratifier la population obtenue pour déterminer le nombre de factures à confirmer.

3) Sélection et édition des lettres de confirmation sur papier à en-tête

Il convient de sélectionner le nombre de factures à confirmer en distinguant les clients de langue anglaise, des clients de langue française et les clients ayant une ou plusieurs factures. Chacune de ces catégories doit être enregistrée dans un fichier distinct afin de faciliter la préparation des courriers.


Confirmation directe des facturations aux clients
Fichier des factures
Stratifier sur les montants et Exclure les factures qui ne sont pas à circulariser
Fichier des factures circularisables
Créer les données nécessaires à l'établissement de la balance âgée
Balance âgée
Stratifier sur les montants
Extraire les factures avec une date d'échéance dépassée de plus de 90 jours
Liste des factures ayant une date d'échéance dépassée de plus de 90 jours
Fichier des factures stratifiées
Déterminer la taille de l'échantillon à circulariser
Fichier des factures sélectionnées
Fichier des adresses clients
Trier sur le numéro du client
Trier sur le numéro du client
Fichier des factures triées
Fichier des adresses clients triées
numéro du client
Rapprochement
Fichier des factures sélectionnées avec les adresses
Cumuler les factures sur le numéro du client
Fichier des factures cumulées
numéro du client
Rapprochement
Extraire les clients ayant une seule facture
Extraire les clients à factures multiples
Cumuler les factures sur le numéro de client
Liste des factures simples sélectionnées pour publipostage
Liste des factures multiples sélectionnées pour publipostage

E. Principaux problèmes rencontrés

- Recoupement avec la comptabilité

La totalisation du fichier des factures peut présenter des écarts par rapport à la comptabilité. L'explication peut résider dans un décalage entre la date de l'extraction et la date de l'arrêté comptable.

- Identifier les pièces à exclure de la base de la confirmation

Les avoirs, les pièces soldées ainsi que les factures intra-groupe doivent être retirés de la base de confirmation. Il est généralement possible de distinguer les avoirs grâce au type de pièce et les pièces soldées grâce à un code de lettrage. En revanche, les pièces intra-groupe sont plus difficiles à identifier. Afin de les éliminer de la sélection, il faut lister les codes clients intra-groupe et rapprocher cette liste de l'ensemble du fichier des factures.

- Identifier les clients à circulariser en anglais

Pour distinguer les clients anglophones des clients francophones, il est possible de s'appuyer sur le champ « Pays » dans le fichier des adresses. Il est utile de demander cette information à l'entreprise lors de l'extraction.

- Fusion rendue délicate par la présence éventuelle de guillemets dans le fichier des adresses

Lors de la préparation des lettres de confirmation sous traitement de textes, via la fusion des fichiers tableur, il faut s'assurer que les caractères spéciaux tels que les guillemets et les accents ont été bien importés. Si ce n'est pas le cas, il faut procéder aux corrections manuellement.

5.2.4. Cycle des Immobilisations

Contrôles possibles :

- les immobilisations brutes,
- les amortissements,
- la mise en service des immobilisations,
- les dates de début d'amortissement.

5.2.5. Cycle de la Paie

Contrôles possibles :

- le calcul des rubriques de paie (rémunération brute, charges patronales, prime d'ancienneté),
- le calcul des droits à congés payés,
- la provision pour congés payés,
- les provisions de fin d'année,
- les indemnités de départ en retraite.

EXEMPLE DE PROGRAMME : VERIFICATION DU CALCUL DES INDEMNITES DE DEPART EN RETRAITE

A. Présentation

Ce programme permet de vérifier le calcul des indemnités de départ en retraite effectué par l'entreprise, selon la norme comptable internationale IAS19. L'engagement est évalué à partir de la formule suivante :

$S * (1+ TXS) * (1+Tp)^{n} * SR * PS * (1+TXA)^{-n} * D$

n	:	nombre d'années jusqu'à la retraite
S	:	salaire mensuel de référence
TXS	:	taux de charges sociales
SR	:	probabilité de présence à la retraite
PS	:	probabilité de survie jusqu'à l'âge de la retraite
TXA	:	taux d'actualisation
Tp	:	taux de progression des salaires
D	:	droits acquis actuellement en mois de salaire

B. Fichiers nécessaires

Les informations nécessaires à la vérification de l'évaluation de l'engagement sont les suivantes :

1) Fiches d'identification des salariés :

- identifiant (matricule, numéro de sécurité sociale, etc.),
- sexe,
- date de naissance,
- date d'entrée dans la société,
- catégorie professionnelle (en accord avec la convention collective),
- salaire annuel de l'exercice incluant toutes les primes récurrentes.

2) Tables de mortalité éditées par l'INSEE.

3) Les données relatives aux droits acquis par les salariés : les conventions collectives définissent les droits d'indemnité de départ en retraite en fonction de la catégorie professionnelle et de l'ancienneté.

4) Les éléments particuliers à l'entreprise :

- taux de charges sociales,
- taux d'actualisation,
- taux de progression des salaires,
- âge du départ en retraite.

C. Réalisation des tests

Les étapes :

1) Obtention des éléments de calcul

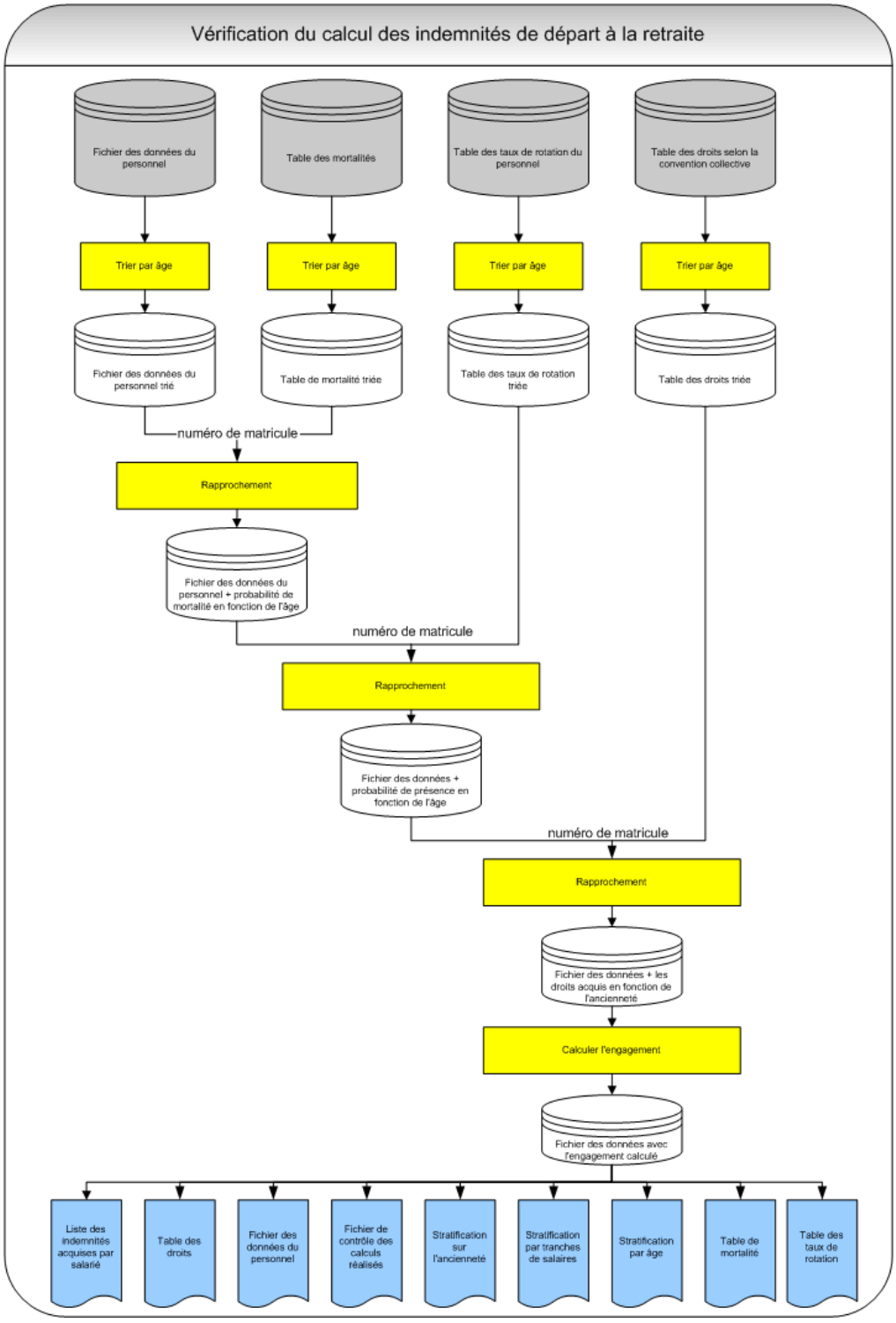
Il convient de mettre en forme le fichier des données individuelles de la façon suivante :

- extraire la liste du personnel,
- retirer de la liste tous les salariés en contrats temporaires : CDD, stagiaires, apprentis, personnel en détachement, etc.,
- calculer un salaire mensuel sur la base de 12 mois (= salaire annuel/12), ne pas tenir compte des parts variables, ne garder que les éléments de rémunération à caractère permanent,
- si besoin, mettre les dates au format JJ/MM/AAAA,
- incorporer les statuts : cadre, agent de maîtrise, employé, etc.

2) Selon le logiciel utilisé, prévoir l'insertion des données suivantes :

- les droits acquis selon l'ancienneté et la convention collective,
- la probabilité de vie jusqu'à l'âge de la retraite,
- la probabilité de présence à l'âge de la retraite en fonction du taux de rotation,

3) Programmer la formule de calcul de l'engagement pour indemnité de départ à la retraite explicitée plus haut.



ANNEXES

Les annexes comprennent notamment des supports opérationnels pouvant être utilisés sur les missions et une étude de cas illustrant la méthodologie de contrôle présentée au chapitre 1.

Les supports opérationnels sont des outils permettant de mettre en œuvre la méthodologie décrite au chapitre 1. Il s'agit de modèles de feuilles de travail et d'exemples correspondant aux contrôles exposés dans la méthodologie. Ils sont présentés par rapport aux étapes de la démarche d'audit :

- orientation et planification de la mission :
  - prise de connaissance de l'informatique dans l'entreprise : modèle de tableau permettant de déterminer l'incidence sur la fiabilité du système d'information, de la stratégie informatique, de la fonction informatique, de l'importance de l'informatique dans l'entreprise, de la complexité du système d'information,
  - description du système d'information de l'entreprise : exemples de cartographies d'applications et techniques, avec tableaux d'inventaire correspondants,
- évaluation des risques et obtention d'éléments probants :
  - incidence de l'environnement informatique sur le risque inhérent : modèle de tableau permettant de déterminer l'incidence sur le risque inhérent de la conception et l'acquisition des solutions informatiques, la distribution et le support informatique, la gestion de la sécurité, la gestion des projets informatiques,
  - formalisation des processus : conseils facilitant la formalisation d'un processus et exemples de représentation,
  - incidence de l'environnement informatique sur le risque lié au contrôle : modèle de tableau permettant de déterminer l'incidence sur le risque lié au contrôle de chaque processus, à partir des assertions sous-tendant l'établissement des comptes,
  - exemple de présentation schématique de la synthèse des risques.

L'étude de cas est proposée pour illustrer la mise en œuvre de la méthodologie par rapport à une petite et moyenne entreprise. Elle utilise à titre d'exemple les supports opérationnels présentés précédemment.

1. ANNEXE 1 : LES SUPPORTS OPERATIONNELS DE MISE EN ŒUVRE DE LA METHODOLOGIE

1.1. ORIENTATION ET PLANIFICATION DE LA MISSION

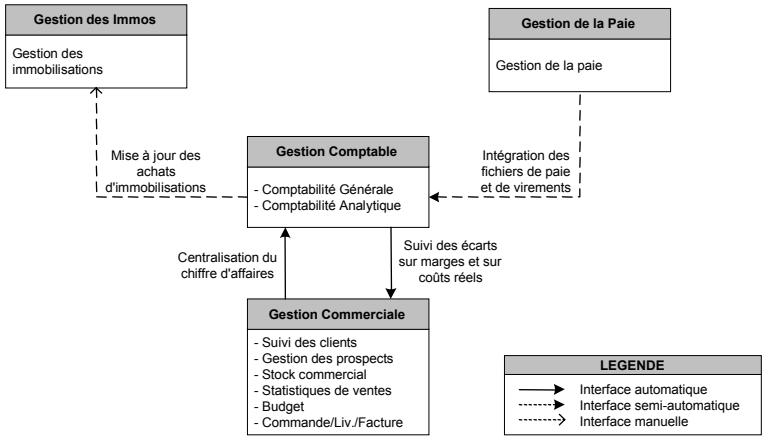
1.1.1. Prise de connaissance de l'informatique dans l'entreprise

Eléments	Description	Incidence sur la fiabilité du système d'information		
		Faible	Modérée	Elevée
Stratégie informatique				
Stratégie élaborée par les entités opérationnelles Sensibilisation de la direction Satisfaction des besoins utilisateurs				
Fonction informatique				
Fonction informatique Organisation informatique Séparation des tâches Externalisation Compétences informatiques Niveau de compétence Charge de travail Niveau de rotation				
Importance de l'informatique dans l'entreprise				
Degré d'automatisation Caractéristiques du système d'information Sensibilité de l'informatique Indisponibilité				
Complexité du système d'information				
Intégration Documentation				

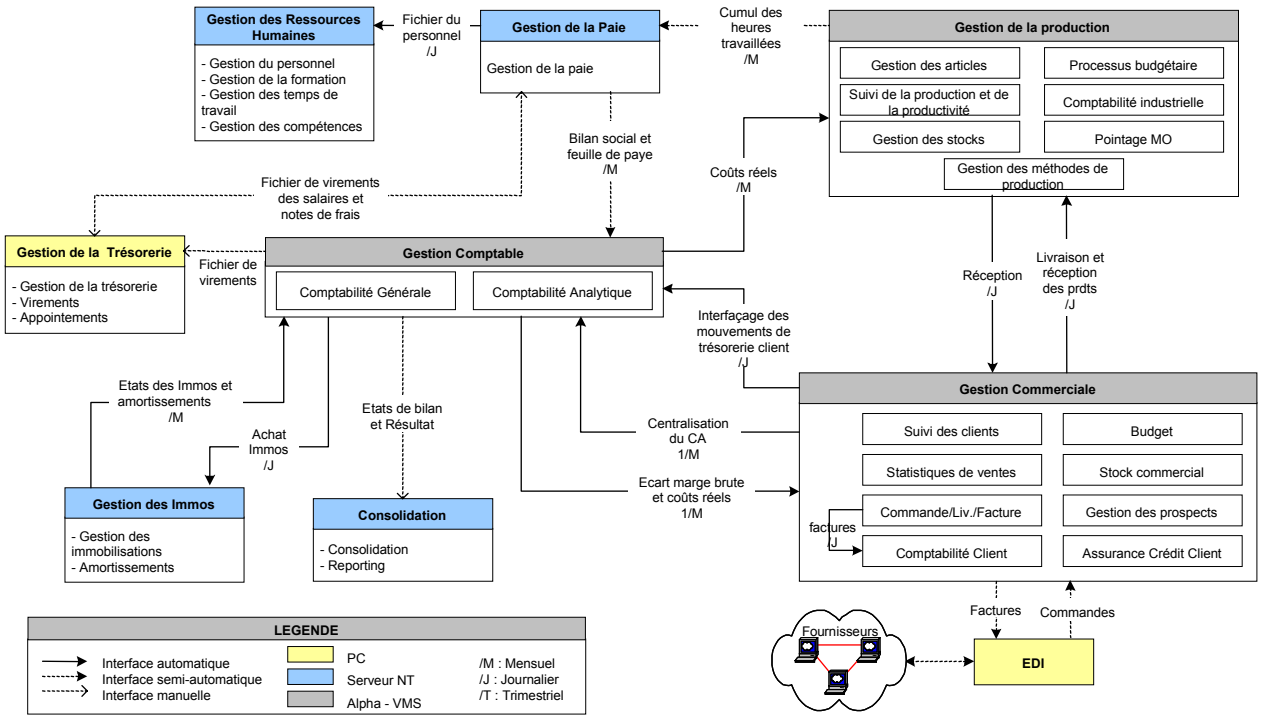
1.1.2. Description du système d'information de l'entreprise

A. Cartographie générale des applications

1) Exemple de système d'information simple



2) Exemple de système d'information complexe



3) Exemples de tableaux d'inventaires de l'architecture informatique de l'entreprise

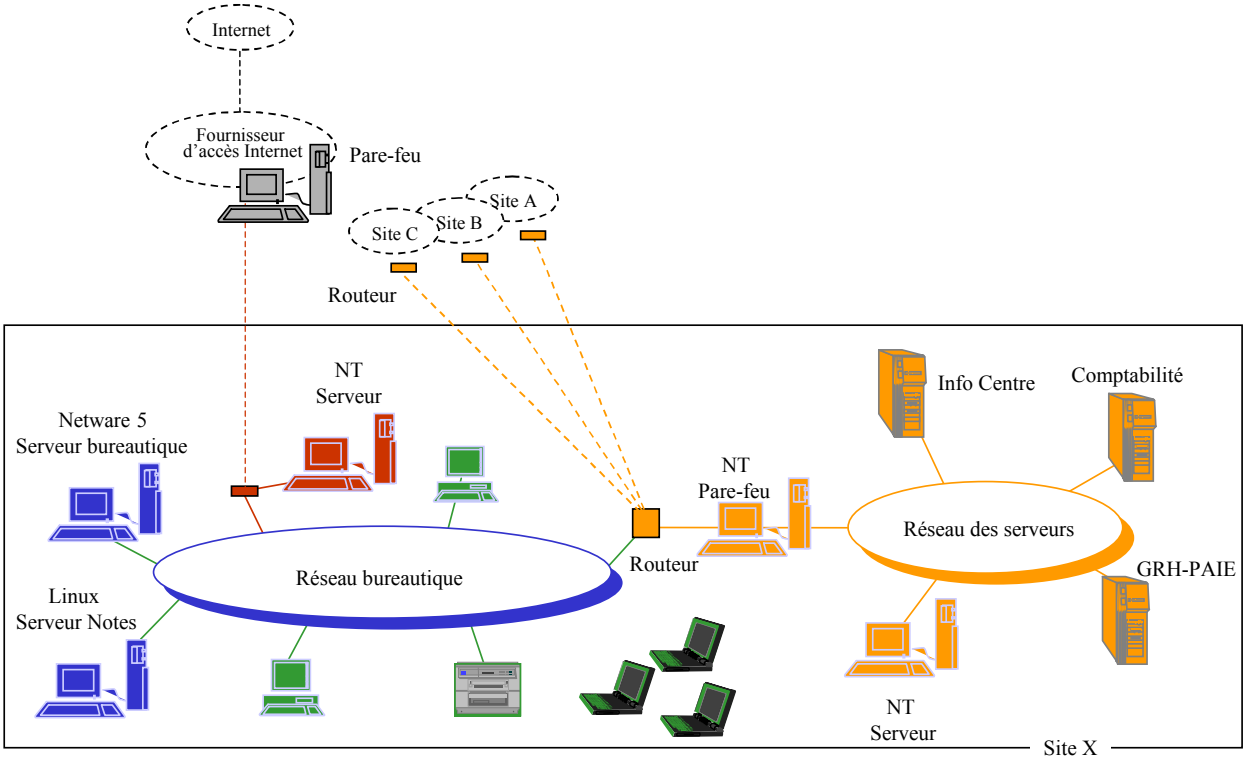
a) Inventaire des principales applications informatiques

Nom de l'application	Type	Principales fonctionnalités	Date de mise en service	Environnement / système d'exploitation	Mode traitement	Editeur / prestataire / Développement interne	Date de modification	Nature des sorties	Estimation du volume traité

b) Inventaire des principales interfaces

Nom de l'interface	Type	Applications Amont / Aval	Nature des flux	Fréquence	Etat des anomalies

B. Exemple de cartographie technique



1) Exemple de tableau d'inventaire des éléments techniques

Site	Service	Serveur		Postes connectés		Postes autonomes		Portables		Imprimantes			Autres	
		Type	Nombre	Système exploitation	Nombre	Système exploitation	Nombre	Système exploitation	Nombre	Communs	Individuels	Caractéris.	Caractéris.	Nombre

1.2. EVALUATION DES RISQUES ET OBTENTION D'ELEMENTS PROBANTS

1.2.1. Incidence de l'environnement informatique sur le risque inhérent

Incidence de l'environnement Informatique sur le risque inhérent	Constats	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs	Communication au gouvernement d'entreprise
Stratégie informatique					
Stratégie élaborée par les entités opérationnelles Sensibilisation de la direction Satisfaction des besoins utilisateurs					
Fonction informatique					
Fonction informatique Organisation informatique Séparation des tâches Externalisation Compétences informatiques Niveau de compétence Charge de travail Niveau de rotation					
Importance de l'informatique dans l'entreprise					
Degré d'automatisation Caractéristiques du système d'information Sensibilité de l'informatique Indisponibilité					
Complexité du système d'information					
Intégration Documentation					
Conception et acquisition des solutions informatiques					
Comment sont achetées et développées les solutions informatiques ? Identification des besoins en nouveaux outils Organisation de la fonction développement / paramétrage Procédures de développement / paramétrage Procédures de tests Comment sont installés et validés les nouveaux systèmes informatiques ?					

Incidence de l'environnement Informatique sur le risque inhérent	Constats	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs	Communication au gouvernement d'entreprise
Tests lors du démarrage de la nouvelle application ou version Validation des développements Niveau de documentation des outils Gestion du changement Comment est assurée la maintenance du système d'information ? Maîtrise du système d'information Maintenance externalisée					
Distribution et support informatique					
Quelle est la qualité du support fourni aux utilisateurs ? Cellule de support (hotline) Manuel utilisateur et documentations disponibles Formations informatiques Comment sont gérés les problèmes d'exploitation quotidiens ? Suivi des performances du système Disponibilité du système Fonction exploitation Historique et surveillance des activités Comment sont gérées les fonctions externalisées ? Procédures de choix des sous-traitants Sous-traitants correspondant aux besoins de l'entreprise Supervision des activités des sous-traitants Contenu des contrats de sous-traitance					
Gestion de la sécurité					
Comment sont gérées les sauvegardes ? Procédure de sauvegarde Modalités de sauvegarde Plan de secours Comment est définie et mise en œuvre la sécurité logique ? Gestion des habilitations / profils utilisateurs Gestion des mots de passe Utilisation d'Internet / messagerie Antivirus					

Incidence de l'environnement Informatique sur le risque inhérent	Constats	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs	Communication au gouvernement d'entreprise
Protection du réseau Sensibilisation des utilisateurs La sécurité physique est-elle satisfaisante ? Moyens d'accès aux locaux Protection incendie Protection électrique					
La gestion des projets informatiques					
Equipe projet Découpage du projet en phases Niveau de documentation Degré d'implication de la direction dans les projets					

NB : Les premières rubriques du tableau (« stratégie informatique », « fonction informatique », « importance de l'informatique dans l'entreprise », « complexité du système d'information ») sont déjà décrites dans la « prise de connaissance de l'informatique dans l'entreprise » et sont analysées ici en termes d'incidence sur le risque inhérent.

1.2.2. Formalisation des processus

Un processus est un « enchaînement de tâches, manuelles, semi-automatiques, automatiques, concourant à l'élaboration, à la production ou au traitement d'informations, de produits ou de services. Exemples : processus de gestion des ventes, processus de gestion des impayés, processus de fabrication, processus d'inventaire permanent, processus d'établissement des comptes, etc. ». (Terme défini par le Comité d'application des normes professionnelles de la CNCC en septembre 2002).

Seuls les processus contribuant directement ou indirectement à la production de l'information comptable et financière sont concernés par la formalisation, l'objectif étant d'identifier les risques liés aux contrôles applicatifs.

Les processus à examiner sont identifiés dans la phase « Orientation et planification de la mission » et sont formalisés dans la phase « Incidence de l'environnement informatique sur le risque lié au contrôle».

L'étude d'un processus nécessite la description des opérations à l'aide d'un diagramme des flux, qui est un schéma montrant l'enchaînement des opérations dans le temps.

A. Les opérations préalables à la formalisation

- Fixer le niveau de détail de la formalisation

Cette étape est fondamentale. Une description trop générale ne permettra pas d'identifier facilement les risques et un niveau trop détaillé peut être un frein à l'analyse et à la lisibilité.
En fonction de la complexité du processus, il pourra être utile de le décomposer en plusieurs sous-processus.

Exemples :

- le processus Achats est composé des sous-processus Gestion fournisseurs, Facturation fournisseurs, Comptabilisation des achats,
- le processus Ventes est composé des sous-processus Gestion client, Facturation client, Comptabilisation ventes,
- le processus Paie est composé des sous-processus Préparation des bulletins de salaire, Etablissement de la paie et édition des bulletins, Comptabilisation de la paie.

- Recenser les informations nécessaires

L'établissement du diagramme des flux nécessite de connaître les éléments suivants :

- les évènements déclencheurs (entrées) et les événements qui en résultent (sorties),
- les traitements (opérations, tâches),
- les acteurs en charge des traitements (département, service, unité organisationnelle, individu…),
- les points de contrôle ou points de décision (connecteurs logiques : OU, ET, CONDITION),
- les interfaces.

1) Les entrées / sorties

Les entrées / sorties peuvent être :
- un document (courrier, formulaire, note, état, commande…),
- un fichier (sur support magnétique ou transmis par voie électronique : EDI, Internet…),
- un appel téléphonique,
- une périodicité, une date,
- un signal,
- …

2) Les traitements

Les traitements sont les programmes informatiques qui utilisent des données et des paramètres pour produire de l'information. Les traitements sont lancés manuellement ou automatiquement.
Exemple : le fichier des commandes est généré par l'application Gestion commerciale contenant un programme, des paramètres et un référentiel qui lui sont propres, à partir des données saisies par l'utilisateur. L'accès à l'application Gestion commerciale n'est possible que pour les utilisateurs autorisés.

3) Les points de contrôles ou de décision

Les contrôles peuvent être automatiques ou manuels (c'est-à-dire effectués par l'utilisateur).

Les contrôles automatiques sont de quatre types :
- les contrôles d'accès à l'application,
- les contrôles à la saisie des données,
- les contrôles des traitements,
- les contrôles des sorties.

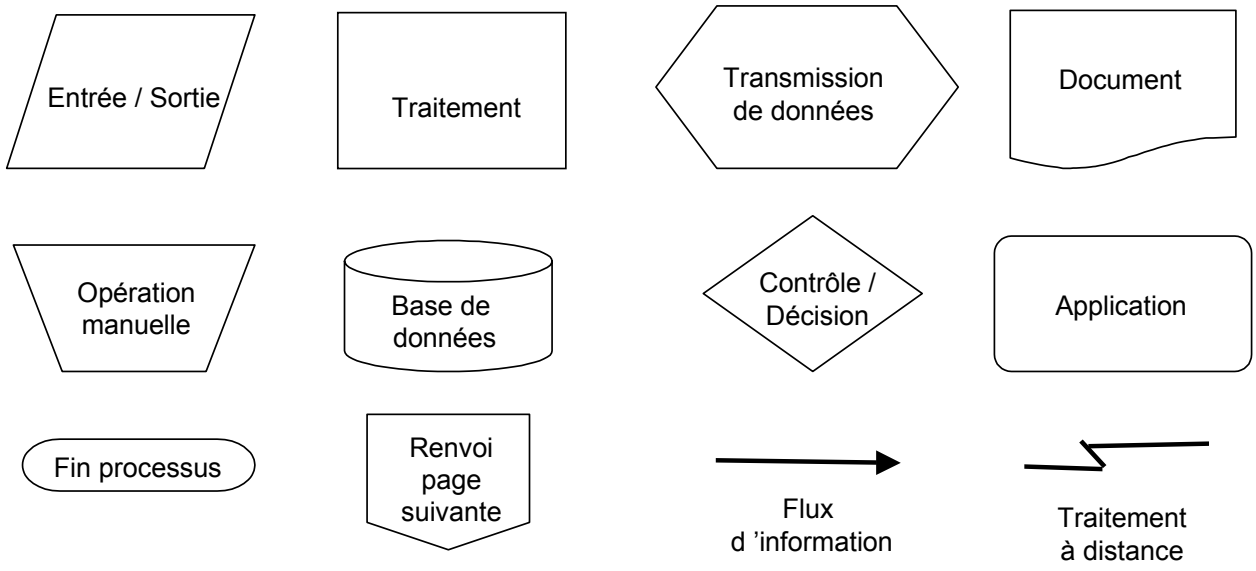
Les contrôles peuvent être effectués au sein d'une application ou entre deux applications (lorsque plusieurs traitements se succèdent appartenant à des applications différentes).

4) Les interfaces

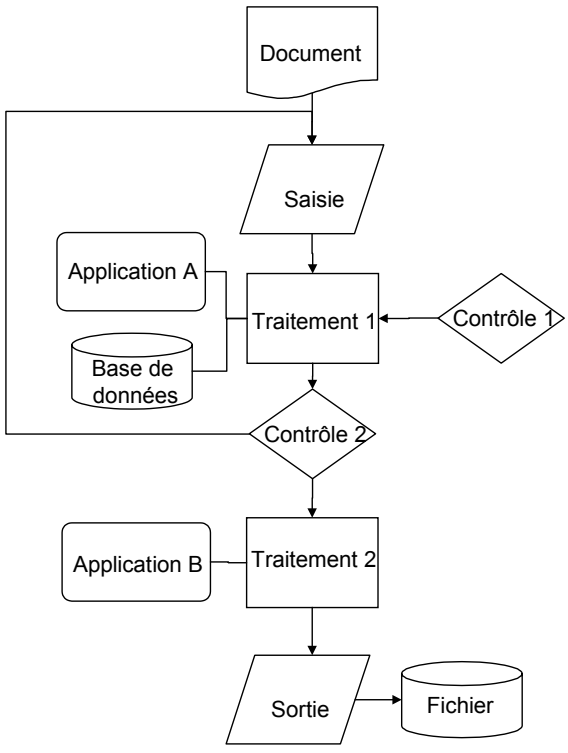
Il s'agit des modalités de communication des données entre plusieurs applications. Les interfaces peuvent être automatiques ou déclenchées manuellement, complètement intégrées aux applications ou nécessiter une intégration de fichiers. Les interfaces représentent un risque d'exhaustivité important dans la mesure où il s'agit de faire communiquer des données entre des applications différentes.

Les contrôles réalisés lors des importations peuvent conduire à des rejets sous la forme de fichiers d'anomalies. Ces fichiers nécessitent obligatoirement un retraitement manuel, lequel s'il n'est pas effectué régulièrement peut avoir des conséquences au niveau des données transférées en comptabilité (rattachement à un mauvais exercice par exemple).

Les symboles les plus souvent utilisés dans un diagramme de flux sont les suivants :



Les composantes élémentaires d'un processus peuvent être schématisées dans le diagramme de flux suivant :



Toutes les informations nécessaires à la formalisation du processus peuvent provenir de la phase « Orientation et planification de la mission », de l'étude de la documentation existante dans l'entreprise, de la connaissance de l'organisation, d'entretiens avec des utilisateurs.

La manière la plus rapide et la plus efficace pour obtenir ces informations est souvent d'organiser des ateliers avec les utilisateurs clés du processus étudié, consistant à formaliser avec eux les diagrammes de flux.

La formalisation en tant que telle peut prendre différentes formes : élaboration de schémas sous forme papier ou électronique. Cette dernière présente l'avantage de pouvoir être archivée dans le dossier de travail dématérialisé et de pouvoir faire l'objet de modifications / ajouts / mises à jour d'une année sur l'autre, par les différents collaborateurs intervenant sur le dossier.

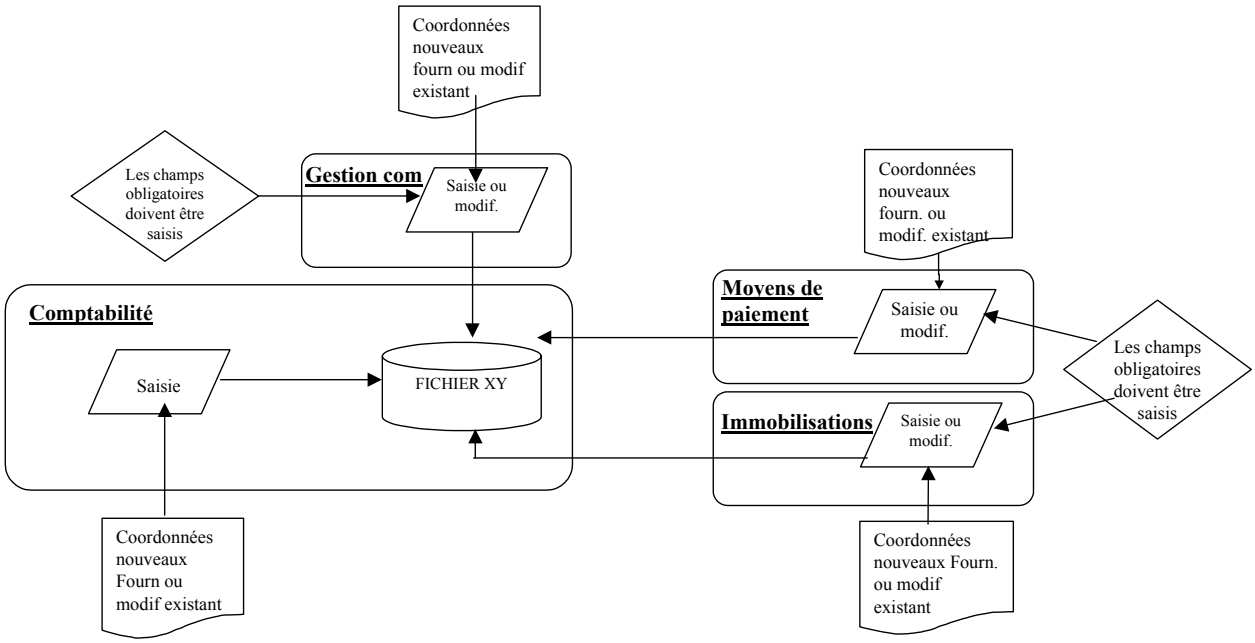
La formalisation électronique peut s'effectuer à partir des fonctionnalités standards disponibles dans la plupart des logiciels bureautiques ou à l'aide de progiciels spécialisés.

L'apport des progiciels spécialisés ne se situe pas tant dans les fonctions graphiques (suffisantes dans les applications bureautiques), que dans la gestion des objets au sein d'une base de données (empêchant l'apparition de doublons et permettant l'utilisation dans plusieurs processus d'un même objet) et la possibilité de connexion avec des logiciels de programmation.

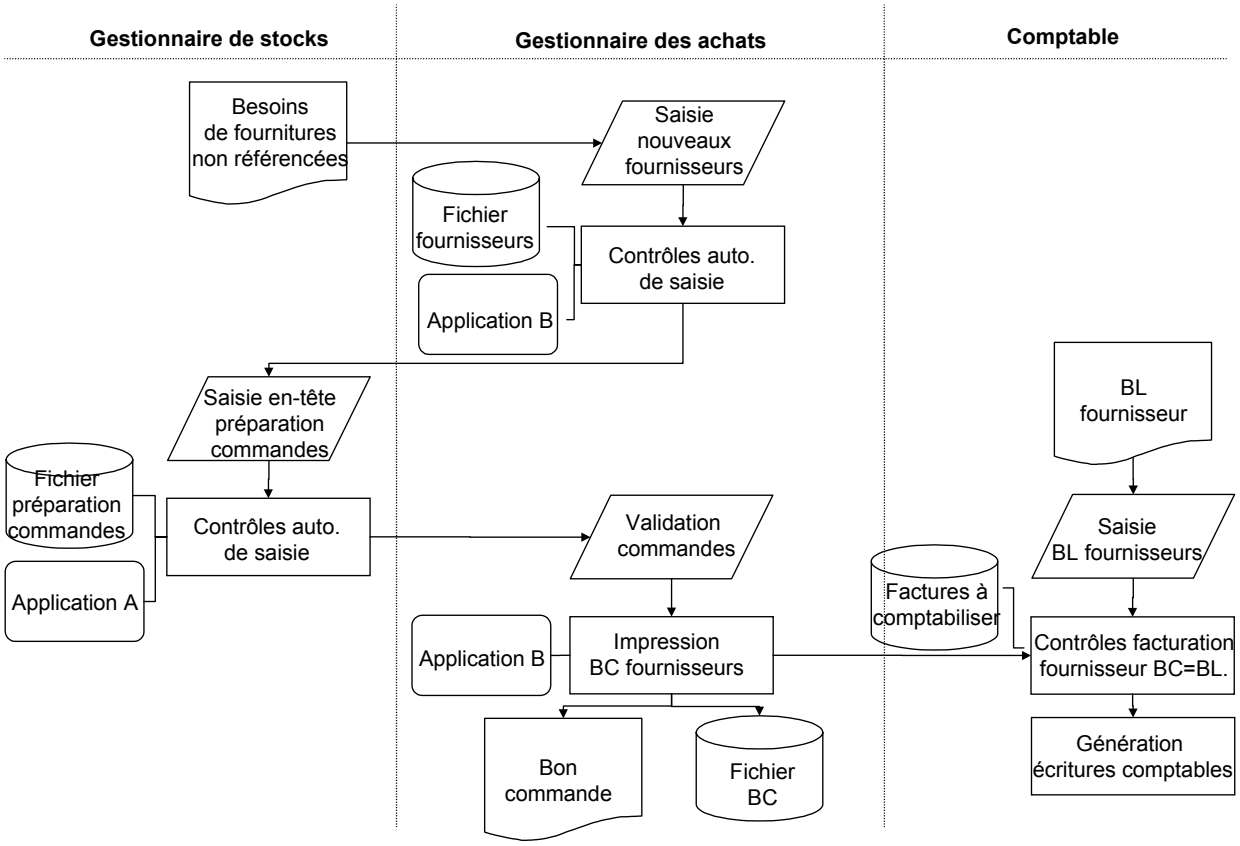
B. Exemples de diagrammes de flux

Il n'existe pas une seule manière de formaliser un diagramme de flux. Les schémas ci-dessous illustrent deux modes de formalisation, le premier mettant en avant l'axe Application, le second l'axe Organisation.

1) Axe Application



2) Axe Organisation

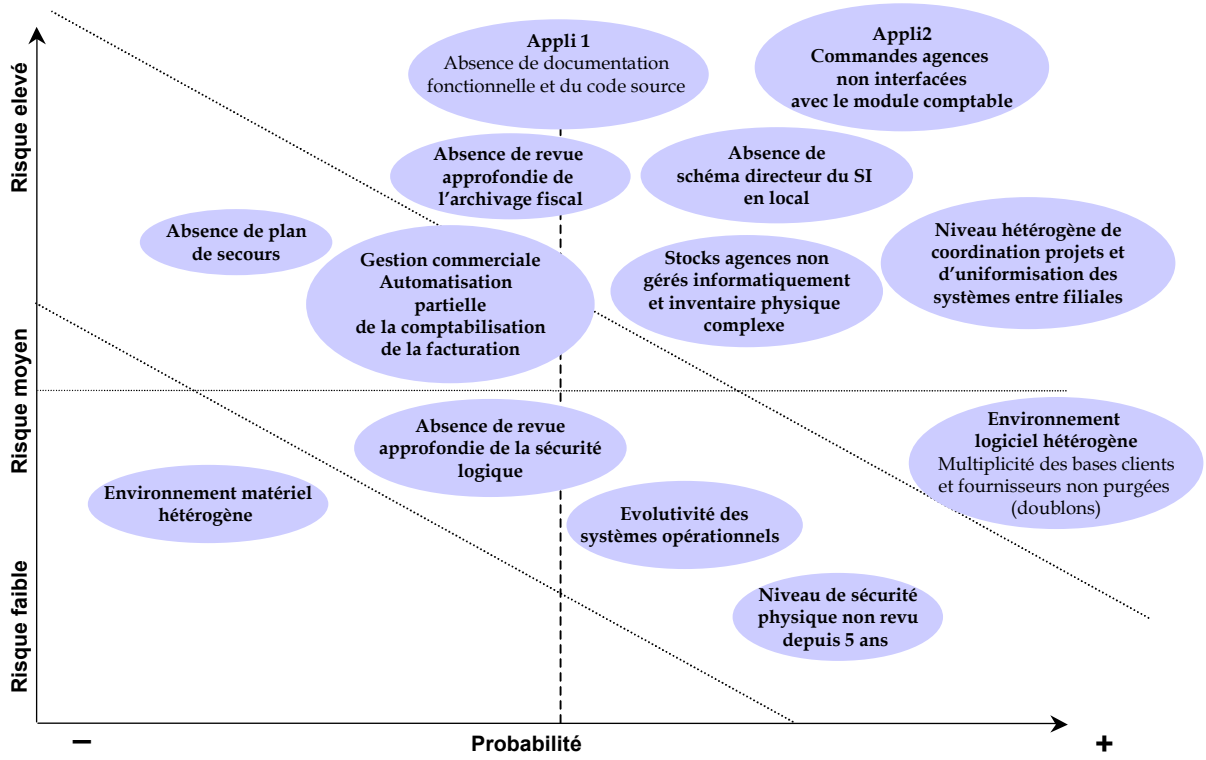


1.2.3. Incidence de l'environnement informatique sur le risque lié au contrôle

Un tableau est à établir par processus :

Assertions	Description du risque théorique	Potentialité du risque théorique	Identification des contrôles (Programmés / utilisateurs)	Appréciation des contrôles internes	Incidence sur le risque lié au contrôle	Recommandations	Impact possible sur les contrôles substantifs	Communication au gouvernement d'entreprise
Existence								
Exhaustivité								
Evaluation								
Mesure								
Rattachement								
Droits et obligations								

1.2.4. Présentation schématique de la synthèse des risques



2. ANNEXE 2 : ETUDE DE CAS

2.1. Présentation

Vous venez d'être nommé commissaire aux comptes de la société Siban. Après une première rencontre avec le P-DG, M. Ding Xian, qui vous a décrit l'activité, vous avez pu rencontrer M. Aloé, directeur financier de la société, également en charge de l'informatique, afin de mieux appréhender le système d'information qui sous-tend les processus de l'entreprise.

Au cours de ces entretiens, vous avez pris les notes suivantes :

- M. Ding Xian, passionné de phytothérapie orientale, a créé il y a 5 ans une boutique de vente de plantes médicinales. En quelques années, le succès de sa boutique lui a permis de s'associer avec M. Aloé, spécialiste des plantes d'Amérique du sud et de créer la société Siban disposant d'une gamme de produits élargie (plantes aromatiques, livres, produits de bien-être, stage de phytothérapie…) et d'un site de ventes sur Internet.

- Suite à d'importantes campagnes marketing, les ventes ont connu une forte augmentation au cours des deux derniers exercices. La société regroupe aujourd'hui plus de 50 personnes et vend en France et à l'étranger.

M. Ding Xian vous expose les faits suivants :

- Il y a deux mois, suite à un désaccord personnel avec M. Ding Xian, M. Ginseng, responsable de l'informatique et présent depuis la création de l'entreprise, a quitté brusquement la société sans laisser de recommandations spécifiques et sans former de successeur. M. Aloé, le directeur financier, a accepté de reprendre la fonction en attendant l'embauche d'une personne plus qualifiée : M. Ding Xian lui fait entièrement confiance ; comme il n'a aucune connaissance en informatique, il ne supervise pas son travail (il n'avait d'ailleurs jamais suivi le travail de M. Ginseng).

- Le schéma directeur informatique date de 5 ans et le plan d'évolution n'a pas été mis à jour depuis 2 ans. M. Ginseng avait l'habitude de gérer seul le parc informatique, mais il est parti sans laisser ses documents de travail.

- Le logiciel de comptabilité utilisé est le même qu'au lancement de la société. La gestion des stocks de produits devient difficile compte tenu du nombre de références à traiter. Le temps de réponse à chaque enregistrement dans le logiciel est extrêmement élevé (parfois plusieurs minutes pour l'enregistrement en brouillard de quelques factures).

- Le projet de migration informatique sur un nouveau progiciel de gestion commerciale et comptabilité est en cours. Certains modules du progiciel sont en phase de test : ils sont accessibles depuis tous les postes de travail afin de permettre des tests en grandeur nature.

- Le projet a été budgété dès son début, à l'acceptation du cahier des charges il y a un an : suite à de nombreux dysfonctionnements, le projet a pris du retard : le budget a été largement dépassé : aucun chiffrage des frais restant à engager n'a été effectué.

- Le service comptabilité regroupe un chef comptable, une personne à mi-temps et des intérimaires lors de la clôture. Lors de la dernière clôture, les trois intérimaires intégrés en urgence n'ont pu être formés, ce qui a entraîné de nombreuses erreurs de traitements. L'un

d'entre eux a même été renvoyé car le volume des fichiers et programmes téléchargés par cette personne ont saturé le réseau informatique.

- Cet incident avait été détecté car M. Ginseng revoyait les logs de connexion et d'anomalies. Depuis son départ, les logs ne sont plus suivis.

- Pour faire une commande, les coordonnées postales et bancaires du client doivent être saisies dans un fichier. Le fichier n'a pas été déclaré à la CNIL et est accessible à tout le personnel de la société (y compris les intérimaires) via le logiciel de gestion commerciale.

- Seuls quelques messages sont envoyés à l'ensemble du personnel pour les mettre en garde contre de nouveaux virus. Le personnel ne dispose pas d'autre formation ou sensibilisation à l'usage du système d'information et à la sécurité informatique. L'antivirus n'est mis à jour qu'une fois tous les trois mois.

- En cas d'indisponibilité du logiciel de gestion des ventes, les répercussions financières et la perte de clientèle pourraient être très significatives. Pourtant, aucun plan de secours n'a été établi.

- La maintenance est assurée par une société extérieure, Indigo, mais les délais d'intervention ne sont pas mentionnés dans le contrat et les informations délivrées par téléphone sont souvent ressenties comme peu satisfaisantes (la société Indigo a développé tous les logiciels utilisés par la société Siban : elle est propriétaire des programmes sources qu'elle a écrits).

- Les habilitations et mots de passe ne sont plus suivis depuis le départ de M. Ginseng. Son mot de passe n'a pas été désactivé et les nouveaux entrants (pour l'instant des stagiaires) utilisent provisoirement un identifiant et un mot de passe commun et connu de tous : « SIBAN ».

- Les locaux informatiques, bureaux et stocks communiquent avec la boutique de ventes au public par une porte non fermée à clé : il arrive que la boutique puisse être sans surveillance à certains moments de la journée. La nuit, l'entreprise est surveillée et les locaux sont sous alarme.

- Les sauvegardes informatiques sont réalisées une fois par semaine et conservées 6 mois dans une armoire fermée dans le local des serveurs informatiques. Les données comptables sont conservées sur cassette pendant 5 ans.

Travaux à réaliser

Appliquer la méthodologie de prise en compte de l'environnement informatique dans la mission d'audit, sachant que seul le processus « Ventes » fera l'objet d'une appréciation au regard du risque lié au contrôle.

2.2. Corrigé indicatif

2.2.1. ORIENTATION ET PLANIFICATION DE LA MISSION

A. Prise de connaissance de l'informatique dans l'entreprise

Eléments	Description	Incidence sur la fiabilité du système d'information		
		Faible	Modérée	Elevée
Stratégie informatique				
Stratégie élaborée par les entités opérationnelles	Le plan directeur date de 5 ans et n'a pas été mis à jour depuis 2 ans + départ du responsable informatique cette année			✓
Sensibilisation de la direction	Le P-DG ne s'occupe pas des aspects informatiques mais le principal associé a en charge la fonction informatique		✓	
Satisfaction des besoins utilisateurs	Peu d'information sur ce thème		✓	
Fonction informatique				
Fonction informatique				
Organisation informatique	Le directeur financier pourtant non spécialisé a toute l'informatique sous sa responsabilité			✓
Séparation des tâches	Pas de séparation des tâches, le travail de M. Aloé n'est pas supervisé			✓
Externalisation	La société Indigo assure la maintenance et est propriétaire des programmes sources des applications			✓
Compétences informatiques				
Niveau de compétence	Des intérimaires travaillent sur les clôtures comptables ; M. Aloé, directeur financier n'a pas de compétences spécifiques en informatique			✓
Charge de travail	Volumes de plus en plus importants à traiter		✓	
Niveau de rotation	Le directeur financier n'a pas de remplaçant prévu en cas d'absence			✓
Importance de l'informatique dans l'entreprise				
Degré d'automatisation	4 applications interfacées entre elles couvrent les principaux processus métier de la société			✓
Caractéristiques du système d'information	Système d'information et architectures simples	✓		
Sensibilité de l'informatique	Fichiers clients avec leurs coordonnées bancaires sont des données sensibles			✓
Indisponibilité	Les applications de gestion commerciale et stock sont indispensables pour mener l'activité de vente de produits			✓
Complexité du système d'information				
Intégration	Toutes les applications sont interfacées entre elles mais certaines interfaces sont entièrement manuelles (architecture simple)		✓	
Documentation	Peu de documentation, l'ancien directeur informatique est parti sans laisser d'instructions		✓	

Conclusion concernant la prise de connaissance de l'environnement informatique

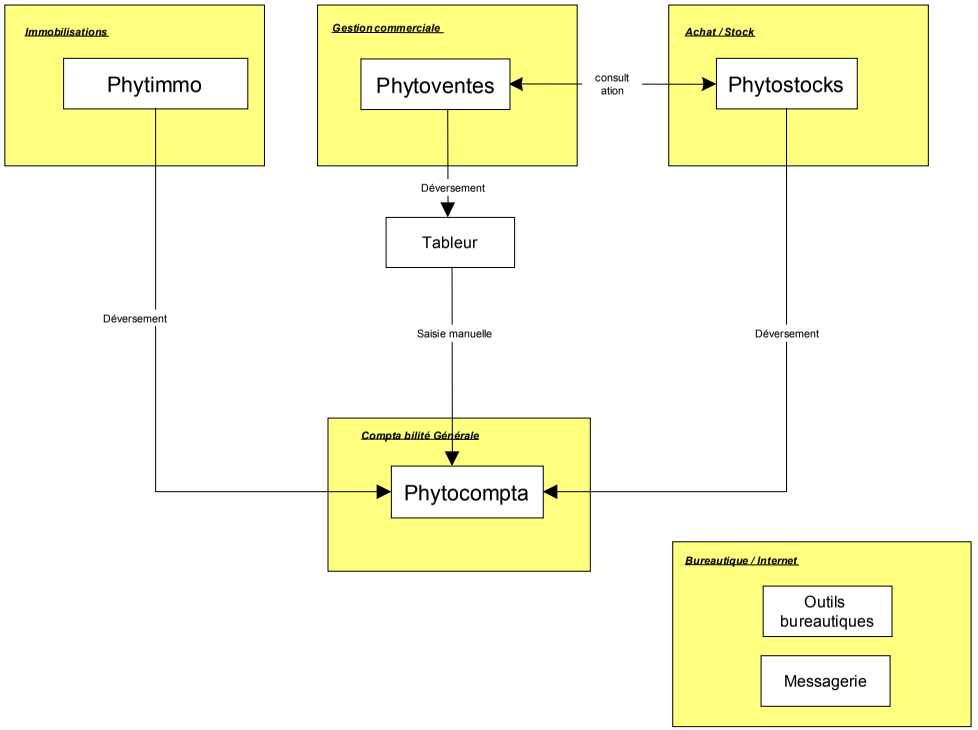
L'incidence de l'environnement informatique sur les opérations de l'entreprise est très significative, en conséquence, il conviendra, lors de l'examen du contrôle interne, de prendre en considération les points suivants :

- la conception et l'acquisition des solutions informatiques,
- la distribution et le support informatique,
- la gestion de la sécurité,
- la gestion des projets informatiques.

B. Description du système d'information de l'entreprise

1) Cartographie générale des applications

Cartographie applicative de Siban



2) Inventaire des principales applications informatiques

Nom de l'application	Type	Principales fonctionnalités	Date de mise en service	Environnement / système d'exploitation	Mode traitement	Editeur / prestataire / Développement interne	Date de modification	Nature des sorties	Estimation du volume traité
Phytimmo	Progiciel	Gestion des immobilisations	1999	Unix	Différé	Editeur Indigo	N/A	Immobilisations	200 immobilisa-tions
Phytoventes	Développement spécifique	Gestion commerciale	1999	Unix	Temps réel	Editeur Indigo	N/A	Factures, marges	10 000 ventes par mois
Phytostocks	Développement spécifique	Gestion des achats et des stocks	1999	Unix	Temps réel	Editeur Indigo	N/A	Stocks, commandes factures	200 références de produits
Phytocompta	Progiciel	Comptabilité générale	1999	Unix	Temps réel	Editeur Indigo	N/A	Ecritures comptables	A préciser

3) Inventaire des principales interfaces

Nom de l'interface	Type	Applications Amont / Aval	Nature des flux	Fréquence	Etat des anomalies
Interface 1	Automatique	Phytoventes / Phytostocks	Ventes	Temps réel	Etat W1
Interface 2	Manuelle	Phytoventes / Phytocompta	Données comptables ventes	Quotidienne	Etat X1
Interface 3	Automatique	Phytimmo / Phytocompta	Données comptables immobilisations	Hebdomadaire	Etat Y1
Interface 4	Automatique	Phytostocks / phytocompta	Données comptables stocks	Quotidienne	Etat Z1

4) Identification des processus à analyser

	Phytovente	Phytostock	Phytimmo	Phytocompta
Processus ventes	✓	✓		
Processus achats		✓		
Processus stocks		✓		
Processus immobilisations			✓	
Processus comptabilité				✓

Conclusion concernant les caractéristiques du système d'information

Le processus Ventes, étant considéré comme le plus sensible, fera l'objet d'une analyse approfondie afin d'identifier les anomalies pouvant avoir une incidence significative sur les comptes ou sur l'information financière diffusée.

C. Prise en compte des aspects informatiques dans le plan de mission

Il est décidé, pour la première année de mandat, d'examiner avec attention le contrôle interne lié à l'informatique. Il sera procédé dans un premier temps à une appréciation de l'incidence de la fonction informatique sur le risque inhérent, puis dans un second temps, à une appréciation de l'incidence de l'application des ventes sur le risque lié au contrôle. Les autres processus Achats, Stocks, Immobilisations, jugés moins critiques feront l'objet d'une prise de connaissance. Leur évaluation approfondie sera réalisée lors des exercices suivants, en conséquence des contrôles substantifs étendus seront réalisés.

Les cas de non respect des textes légaux et réglementaires identifiés sont les suivants :
- fichier clients non déclaré à la CNIL,
- obligations d'archivage fiscal non satisfaites.

2.2.2. Evaluation des risques

A. Incidence de l'environnement informatique sur le risque inhérent

Une matrice est proposée afin d'apprécier l'incidence de l'environnement informatique sur le risque inhérent. Pour chaque élément, sont précisées l'incidence sur la nature et l'étendue des contrôles substantifs à mettre en œuvre et sur la communication au gouvernement d'entreprise.

Incidence de l'environnement informatique sur le risque inhérent	Constat	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
Stratégie informatique					
Stratégie élaborée par les entités opérationnelles	M. Ginseng, le directeur informatique de Siban depuis 5 ans a quitté la société sans assurer sa succession. M. Aloé, directeur financier, a repris la fonction de directeur informatique en attendant l'embauche d'un spécialiste, mais ne contrôle pas encore tous les processus.	Risque de perte du contrôle de certains processus. Risque de perte d'informations connues de l'ancien directeur informatique.	Effectuer un état de l'existant, identifier l'ensemble des procédures existantes ou à mettre en place.	-	Oui
Sensibilisation de la direction	Le schéma directeur informatique date de 5 ans et le plan d'évolution n'a pas été mis à jour alors que l'activité de la société est en pleine évolution. Le directeur informatique est parti sans laisser ses documents de travail et le P-DG ne s'est jamais impliqué dans ses travaux.	Risque de perte de cohérence dans l'évolution du système d'information si le plan d'évolution n'est pas tenu à jour. Le schéma directeur, obsolète risque de ne plus être en adéquation avec les besoins de la société.	Mener une réflexion sur une évolution cohérente du système d'information. Créer un nouveau schéma directeur avec une architecture informatique cible. Définir le plan d'évolution pour les exercices à venir.	-	Oui
Satisfaction des besoins utilisateurs	Aucune information sur ce thème.	-	-	-	-
Fonction informatique					
Fonction informatique **Organisation informatique** **Séparation des tâches**	Le directeur informatique, M. Ginseng et M. Aloé à présent, est seul à s'occuper de tous les aspects informatiques de la société. Le P-DG, M. Ding Xian, ne supervise pas son travail par manque de connaissance technique.	Trop de fonctions assurées par une même personne. Pas de supervision extérieure.	Affecter une ressource à la fonction informatique ou externalisation de la fonction développement chez un prestataire.	Réaliser des tests plus précis afin de s'assurer de l'absence de fraudes	Oui

Incidence de l'environnement informatique sur le risque inhérent	Constat	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
Externalisation	La maintenance et le développement de l'ensemble des logiciels de Siban sont externalisés chez le prestataire Indigo. Cette société est propriétaire des programmes sources des applications développées.	Dépendance trop importante vis-à-vis de la société d'externalisation. Difficultés pour changer de prestataire en cas de mécontentement sur les prestations fournies ou de faillite du prestataire.	S'assurer de la fiabilité de Indigo. Etudier des solutions permettant d'assurer la continuité du système d'information en cas de défaillance d'Indigo.	-	Oui
Compétences informatiques					
Niveau de compétence	Le nouveau responsable des systèmes d'information n'a aucune connaissance en informatique.	Perte de maîtrise du système d'information.	Former le directeur informatique.	-	Oui
Charge de travail	Pas d'information sur ce thème.	-	-	-	-
Niveau de rotation	Faible niveau de rotation, mais le responsable informatique vient de quitter la société.	Perte de maîtrise du système d'information.	-	-	-
Conception et acquisition des solutions informatiques					
Comment sont achetées et développées les solutions informatiques ?					
Identification des besoins en nouveaux outils	Pas d'information sur ce thème.	-	-	-	-
Organisation de la fonction développement/paramétrage	Le développement est externalisé auprès de la société Indigo.	Perte de maîtrise du système d'information.	S'assurer que la société garde la maîtrise de ses systèmes d'information malgré l'utilisation de prestataires.	-	Oui
Procédures de développement et de paramétrage	N/A.	-	-	-	-
Comment sont installés et validés les nouveaux systèmes informatiques ?					
Tests lors du démarrage de la nouvelle application ou version	Les modules en phase de test sont accessibles dans un environnement de production sur tous les postes.	Risque que des écritures de tests soient enregistrées dans le système et ne soient pas effacées lors du déploiement.	Créer un environnement de test spécifique. Ne donner aux développeurs que l'accès à cet environnement.	Oui	Fonction des résultats des tests substantifs menés au final

Incidence de l'environnement informatique sur le risque inhérent	Constat	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
		Les développeurs (Indigo) ont accès à l'environnement de production et peuvent accéder à l'ensemble des données du système.			
Validation des développements	Pas d'information sur ce thème.	-	-	-	-
Niveau de documentation des outils	Pas d'information sur ce thème.	-	-	-	-
Gestion du changement	Pas d'information sur ce thème.	-	-	-	-
Comment est assurée la maintenance du système d'information ?					
Maîtrise du système d'information	M. Ginseng est parti sans avoir assuré la transition auprès du nouveau responsable.	Risque de perte de maîtrise du système d'information.	M. Aloé, qui reprend la gestion informatique, devra se mettre en relation avec le prestataire Indigo afin de reprendre en main le système d'information.	-	Oui
Maintenance externalisée	La maintenance du système est externalisée auprès d'une société qui est propriétaire des programmes sources.	Si la société Siban souhaite changer de prestataire et faire évoluer le système, elle rencontrera de grandes difficultés car elle ne détient pas les programmes sources.	Négocier avec la société prestataire une acquisition des programmes sources et être vigilant lors de l'acquisition ou le développement des futures applications.	-	Oui
Distribution et support informatique					
Quelle est la qualité du support fourni aux utilisateurs ?					
Cellule d'assistance (hot line)	Pas de hot line.	Peu de risque étant donné la taille de l'entreprise.	-	-	-
Manuel utilisateur et documentations disponibles	Pas d'information sur ce thème.	-	-	-	-

Incidence de l'environnement informatique sur le risque inhérent	Constat	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
Formations informatiques	Le personnel du service comptabilité n'a reçu aucune formation à l'informatique. Les intérimaires ne sont pas formés à l'utilisation du logiciel comptable.	Risques de mauvaise utilisation des applications. Risques d'erreurs, de perte de temps...	Demander au personnel les formations qu'il souhaite suivre. Organiser des formations de sensibilisation à l'informatique et aux applications dont ils ont l'utilisation. Des formations seront à mettre en place pour le déploiement du nouveau logiciel.	-	Oui
Comment sont gérés les problèmes d'exploitation quotidiens ?					
Suivi des performances du système	Revue régulière des listings d'exploitation et de contrôle. Des listings de connexion et d'anomalie existent mais ils ne sont pas régulièrement revus.	Non détection de tentatives d'intrusion non autorisées. Non détection de dysfonctionnements dans les interfaces ou dans les traitements automatisés internes au système d'information. Non détection de modifications injustifiées dans les bases tarifs ou clients.	Fixer une procédure de revue et de conservation des listings de connexions, de contrôles et d'anomalies par le responsable de l'exploitation du système d'information.	Oui	Des anomalies constatées lors des interfaces pourraient mettre en évidence la non exhaustivité des comptes
Disponibilité du système	Les temps de réponse de l'application de gestion des stocks sont très élevés.	Perte de temps.	Supprimer les références en stock qui ne sont plus utilisées. Envisager d'augmenter la capacité de la base de données gérant les stocks.	-	Oui
Fonction exploitation	La fonction est assurée par le directeur informatique	Non séparation de fonctions.	Former une ou plusieurs personnes à la fonction exploitation.	-	Oui
Historique et surveillance des activités	Pas d'information sur ce thème.	-	-	-	-
Comment sont gérées les fonctions externalisées					
Procédures de choix des sous-traitants	Pas d'information sur ce thème.	-	-	-	-
Sous-traitants correspondant aux besoins de l'entreprise	Les délais d'intervention et la qualité des renseignements fournis par Indigo sont jugés non satisfaisants par les utilisateurs.	Faible risque de perte de temps.	Renégocier le contrat avec Indigo pour obtenir une amélioration de la qualité de service.	-	Oui

Incidence de l'environnement informatique sur le risque inhérent	Constat	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
Supervision des activités des sous-traitants	Pas d'information sur ce thème.	-	-	-	-
Contenu des contrats de sous-traitance	Pas d'information sur ce thème.	-	-	-	-
Gestion de la sécurité					
Comment sont gérées les sauvegardes ?					
Procédure de sauvegarde et modalités de sauvegarde	Procédures de sauvegardes correctes, cependant les sauvegardes ne sont pas faites en double et effectuées régulièrement.	En cas d'incendie ou dégât des eaux dans les locaux de l'entreprise, les sauvegardes peuvent être perdues sans pouvoir reconstituer les données contenues dans les cassettes. Risque que les données ne puissent être relues. La fréquence des sauvegardes n'est pas assez importante.	Garder une seconde sauvegarde dans un lieu extérieur à la société. Effectuer des tests de relecture sur des cassettes prises au hasard. Mettre en place une procédure quotidienne de sauvegarde automatique des données.	-	Oui
Plan de secours	Il n'existe pas de plan de secours. De plus, le contrat de prestation externe avec Indigo ne précise pas de délais d'intervention. La prestation de Indigo ne satisfait pas les utilisateurs.	Risque d'indisponibilité longue du SI en cas d'incident. Risque de difficultés d'exploitation car la disponibilité du serveur est importante pour l'activité de la société.	Renégocier le contrat de maintenance en précisant les délais maximums d'intervention. Changer de société de maintenance si les solutions proposées ne semblent pas satisfaisantes.	-	Oui
Comment est définie et mise en œuvre la sécurité logique ?					

Incidence de l'environnement informatique sur le risque inhérent	Constat	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
Gestion des habilitations / profils utilisateurs	Pas de politique de gestion de profils au sein des applications. L'ensemble du personnel disposant d'un mot de passe a accès à l'ensemble des données du SI en lecture et modification.	Risque de fraude et d'erreurs d'utilisation (possibilité de modification des tarifs pour un client donné, puis effacement de la modification). Confidentialité des données non garantie (les intérimaires ayant également accès à l'ensemble des données).	Créer des profils selon la fonction occupée au sein de la société.	-	Oui
Gestion des mots de passe	Les habilitations et mots de passe ne sont plus suivis depuis deux mois : le mot de passe de M. Ginseng n'a pas été désactivé. Un mot de passe commun est utilisé pour les nouveaux entrants : l'identifiant égal au mot de passe « Siban » est trop facile à trouver.	Risque d'accès et de modification non autorisés à des données confidentielles (risque d'autant plus important que le système d'information de Siban contient des données sensibles comme les coordonnées bancaires de la base clients). Risques de fraude par M. Ginseng : il est parti en désaccord avec la direction et connaît parfaitement le SI de Siban.	Imposer des mots de passe de plus de 5 caractères, ne correspondant pas à des mots du dictionnaire ou des prénoms, avec alternance de chiffres et de lettres et à changer régulièrement. Les mots de passe communs à plusieurs utilisateurs sont à éviter. Reprendre la gestion des habilitations et désactiver les identifiants des personnes ayant quitté la société.	-	Oui
Utilisation d'Internet / messagerie	Pas d'information sur ce thème.	-	-	-	-
Antivirus	L'antivirus est mis à jour tous les trois mois.	De nouveaux virus peuvent ne pas être détectés et infecter le système d'information.	Mettre à jour l'antivirus une fois par semaine.	-	Oui
Sensibilisation des utilisateurs	Le personnel reçoit des courriels de mise en garde contre des virus informatiques. Un intérimaire a été renvoyé pour avoir trop téléchargé de fichiers.	Risque de perte de données pour cause de virus. Une mauvaise utilisation du système d'information peut entraîner des pertes de données et une indisponibilité du réseau.	Rédiger et faire signer à l'ensemble du personnel une charte de bonne utilisation du SI. Verrouiller les postes de travail.	-	Oui

Incidence de l'environnement informatique sur le risque inhérent	Constat	Incidence sur le risque inhérent	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
La sécurité physique est-elle satisfaisante ?					
Moyens d'accès aux locaux	Toute personne peut avoir accès aux salles machines et bureaux en passant par la boutique. De nuit, une alarme et un gardien sécurisent les accès.	Risque de fraude ou d'accès non autorisés à des données confidentielles si une personne mal intentionnée accède aux locaux informatiques.	Accompagner les visiteurs de leur entrée à leur sortie de l'entreprise. Surveiller en permanence les accès aux locaux. Fermer la porte d'accès entre la boutique et les locaux informatiques.	-	Oui
Protection incendie	Pas d'information sur ce thème.	-	-	-	-
Protection électrique	Pas d'information sur ce thème.	-	-	-	-
La gestion des projets informatiques					
Equipe projet	Pas d'information sur ce thème.	-	-	-	-
Découpage des projets en phases	Pas d'information sur ce thème.	-	-	-	-
Niveau de documentation	Pas d'information sur ce thème.	-	-	-	-
Degré d'implication de la direction dans le projet	Pas d'information sur ce thème.	-	-	-	-

(1) L'impact définitif sur les contrôles substantifs est à apprécier en relation avec l'évaluation du risque lié au contrôle.

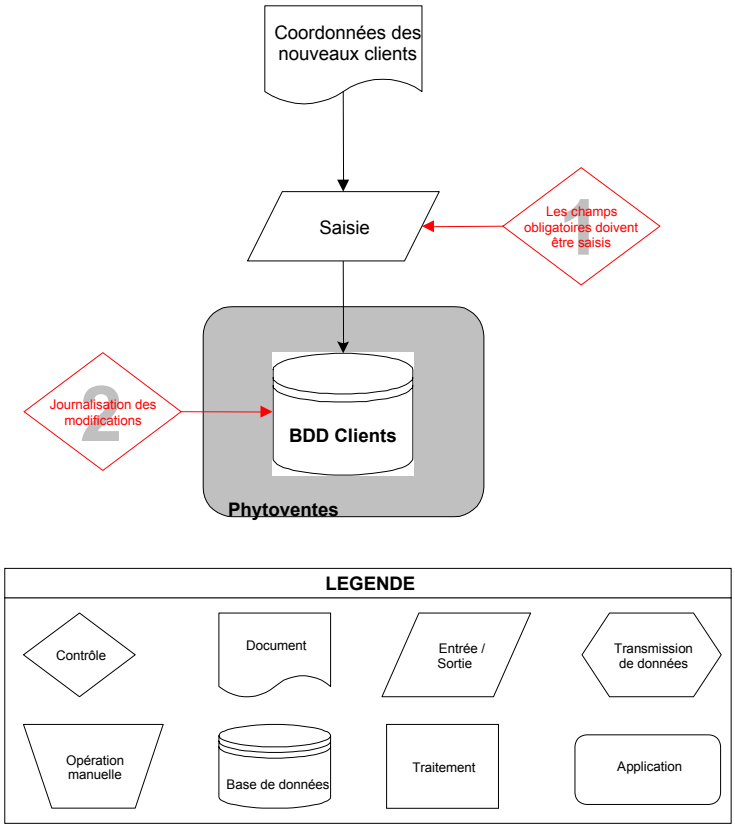
B. Incidence des contrôles applicatifs sur le risque lié au contrôle

1) Description du processus

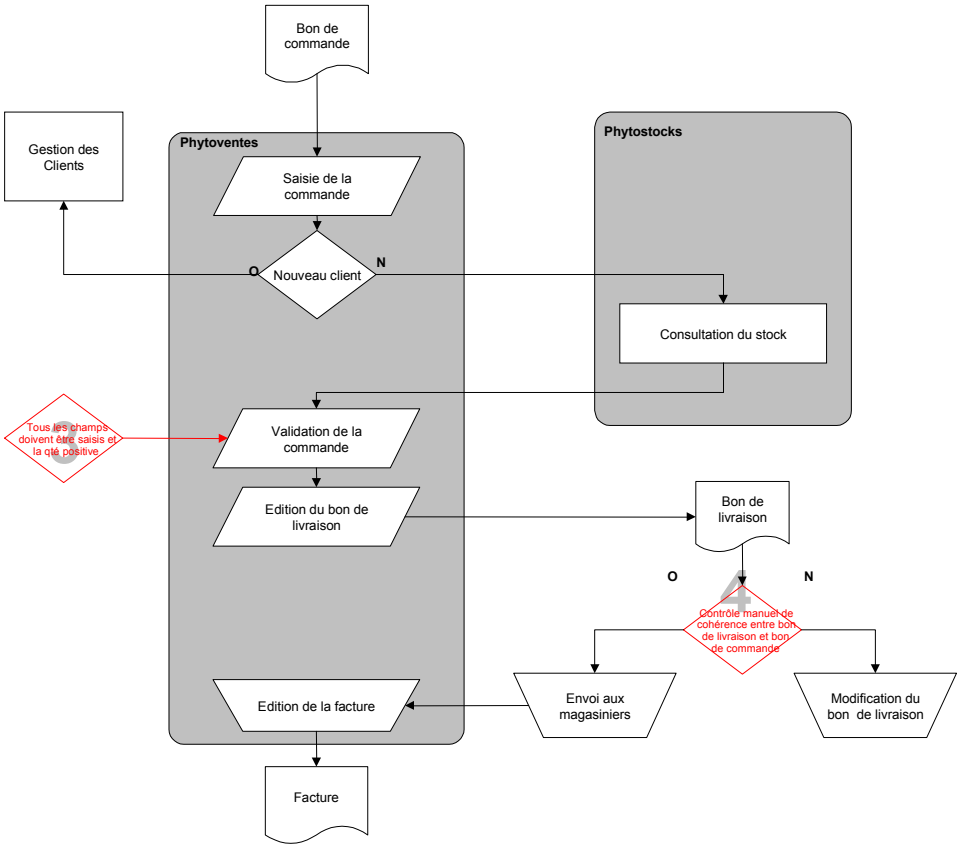
Le processus « Ventes » se décompose en trois sous-processus :

- la gestion des clients,
- la gestion des commandes,
- la comptabilisation des factures.

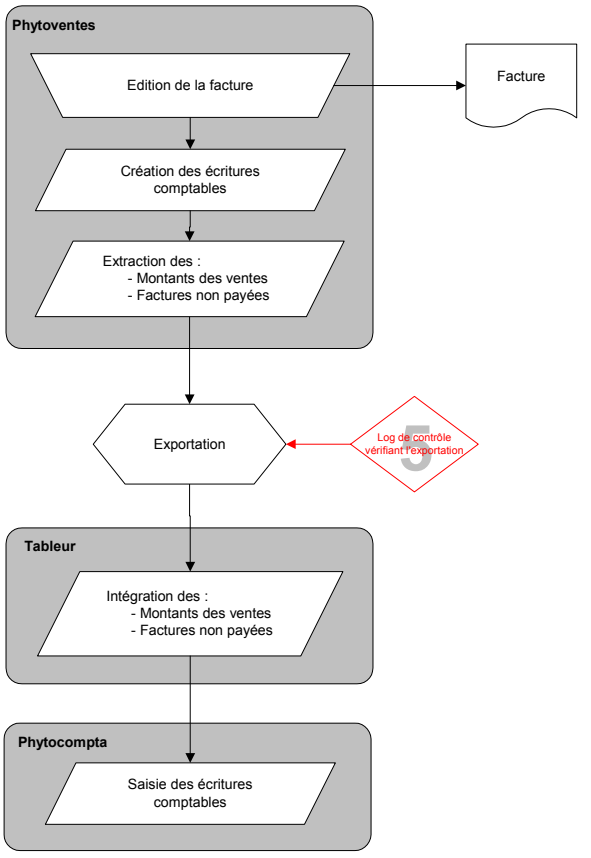
a) La gestion des clients



b) La gestion des commandes



c) La comptabilisation des factures



2) Incidence sur le risque lié au contrôle : analyse du processus « Ventes »

(CX) correspond au numéro du contrôle identifié sur les diagrammes de flux.

Assertions	Description du risque théorique	Potentialité du risque théorique	Identification des contrôles (Programmés / utilisateurs)	Appréciation des contrôles internes	Incidence sur le risque lié au contrôle	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
Gestion des clients								
Exhaustivité	Suppression de données clients ou tarifaires compte tenu de l'absence de restriction d'accès à la base Clients.	Modérée	(C2) Les modifications réalisées sur la base des clients avec le nom de l'auteur de la modification sont journalisées. Le journal n'est pas systématiquement analysé.	Mauvaise	Modérée	Mise en place d'une procédure de revue périodique du journal des modifications.	-	-
Evaluation	Erreur de saisie des données clients et des paramétrages qui leur sont attachés (code TVA, ristournes…).	Modérée	(C1) La fiche client n'est enregistrée que si tous les champs obligatoires sont saisis. (C2) Les modifications réalisées sur la base des clients avec le nom de l'auteur de la modification sont journalisées. Le journal n'est pas systématiquement analysé.	Moyenne	Faible	-	-	-
Evaluation	Modification de données clients ou tarifaires compte tenu de l'absence de restriction d'accès à la base Clients.	Elevée	(C2) Journalisation des modifications réalisées sur la base des tarifs avec le nom de l'auteur de la modification. Le journal n'est pas systématiquement analysé.	Mauvaise	Elevée	Mise en place d'une procédure de revue périodique du journal des modifications.	-	-
Gestion des commandes								
Evaluation	Erreurs dans la saisie des commandes.	Modérée	(C3) Contrôles automatiques dans le masque de saisie des commandes : ▪ Champs obligatoires renseignés, ▪ Montant de la facture	Moyenne	Faible	-	-	-

Assertions	Description du risque théorique	Potentialité du risque théorique	Identification des contrôles (Programmés / utilisateurs)	Appréciation des contrôles internes	Incidence sur le risque lié au contrôle	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
			positif.					
Evaluation	Envoi de la facture sans livraison.	Modérée	Aucun	-	Modérée	Définition d'une procédure visant à informer la comptabilité des livraisons envoyées.	Oui	Fonction des résultats des tests substantifs menés au final
Evaluation	Erreur dans les bons de livraison.	Modérée	(C4) Contrôle manuel de cohérence systématique entre le bon de commande et le bon de livraison.	Moyenne	Faible	-	-	-
Existence	Bon de livraison ne correspondant à aucune commande.	Modérée	Édition automatique du bon de livraison après la validation de la commande.	Bonne	Faible	-	-	-
Exhaustivité	Commande non suivie d'un bon de livraison.	Modérée	Édition automatique du bon de livraison après la validation de la commande.	Bonne	Faible	-	-	-
Exhaustivité	Envoi de la livraison sans facture (bon de livraison n'entraînant pas de facturation).	Élevée	Aucun	Mauvaise	Elevée	Définition d'une procédure visant à s'assurer que l'ensemble des livraisons est envoyé avec une facture.	-	-
Rattachement	Comptabilisation de la facture sur la mauvaise période (non synchronisation de la facturation et de la livraison).	Modérée	Aucun	Mauvaise	Modérée	Définition d'une procédure permettant de s'assurer que l'ensemble des factures a bien été comptabilisé avant la clôture de la période comptable concernée.	Oui	Fonction des résultats des tests substantifs menés au final
Comptabilisation des factures								
Exhaustivité	Une facture n'entraîne pas la création d'écritures comptables.	Élevée	Création automatique des écritures comptables dès l'édition des factures.	Bonne	Faible	-	-	-
Exhaustivité	Perte de données au niveau de l'interface entre	Modérée	(C5) Revue de l'édition de l'état de contrôle par le responsable de l'interface.	Moyenne	Faible	-	-	-

Assertions	Description du risque théorique	Potentialité du risque théorique	Identification des contrôles (Programmés / utilisateurs)	Appréciation des contrôles internes	Incidence sur le risque lié au contrôle	Recommandations	Impact possible sur les contrôles substantifs (1)	Communication au gouvernement d'entreprise
	Phytoventes et le tableur.							
Exhaustivité	Erreurs de saisie des chiffres du tableur dans le logiciel comptable.	Élevée	Aucun	Mauvaise	Élevée	Mise en place d'une interface automatique entre l'application Phytoventes et l'application Phytocompta.	Oui	Fonction des résultats des tests substantifs menés au final
Evaluation	Altération des données au niveau de l'interface avec le tableur.	Modérée	(C5) Revue de l'édition de l'état de contrôle par le responsable de l'interface.	Moyenne	Faible	-	-	-
Evaluation	Erreurs de saisie des chiffres du tableur dans le logiciel comptable.	Élevée	Aucun	Mauvaise	Élevée	Mise en place d'une interface automatique entre l'application Phytoventes et l'application Phytocompta.	Oui	Fonction des résultats des tests substantifs menés au final

(1) L'impact définitif sur les contrôles substantifs est à apprécier en relation avec l'évaluation du risque inhérent.

2.2.3. Obtention d'éléments probants

A. Synthèse de l'évaluation des risques

L'analyse des risques des processus informatiques a permis de dégager les points suivants :

- stratégie informatique :
  - l'absence d'une stratégie à long terme concernant le système d'information peut entraîner un décalage entre les fonctionnalités offertes par le système et les besoins réels des utilisateurs,
- fonction informatique :
  - l'absence d'une personne spécialisée en charge des questions informatiques et une externalisation non suffisamment maîtrisée peuvent entraîner à terme une perte de contrôle de certains processus,
- conception et acquisition des solutions informatiques :
  - la non séparation entre l'environnement de tests et l'environnement de production peut être à l'origine d'anomalies au niveau des données présentes dans le système,
  - des difficultés à faire évoluer le système en cas de changement de prestataire, la société Siban n'étant pas propriétaire des codes sources,
- distribution et support informatique :
  - manque de formation du personnel pouvant être à l'origine d'une mauvaise utilisation du système et d'erreurs de saisie,
  - faiblesses dans la gestion des problèmes d'exploitation pouvant être à l'origine de non détection d'intrusions, de dysfonctionnement dans les interfaces et les traitements,
- gestion de la sécurité :
  - pertes de données possibles en raison de faiblesses dans la gestion des sauvegardes,
  - fraudes ou erreurs possibles en raison d'une absence de gestion des habilitations.

L'analyse des risques du processus « Ventes » a permis de dégager les points suivants :

- l'absence de contrôle suite à la saisie manuelle des écritures de ventes dans Phytocompta ne permet pas de garantir l'exhaustivité des écritures enregistrées en comptabilité,
- l'absence de politique de gestion des droits d'accès pourrait remettre en cause l'exactitude des tarifs produits. L'historisation des actions utilisateurs ne suffit pas à garantir l'intégrité des données,
- dans la situation actuelle, une facture pourrait être enregistrée sur l'exercice N alors que la livraison n'interviendra que sur l'exercice N+1.

B. Contrôles substantifs

Des contrôles substantifs doivent être réalisés. Il s'agit pour l'essentiel de travaux d'analyse de données consistant à comparer les informations enregistrées dans l'application Phytoventes avec celles enregistrées dans l'application Phytocompta, afin de s'assurer de l'exhaustivité et de la correcte évaluation des enregistrements des factures :

- vérifier que l'environnement de production ne contient pas de données erronées provenant des jeux de tests,
- identifier les anomalies potentielles au niveau des connexions,
- vérifier l'existence de factures envoyées sans livraisons correspondantes,
- vérifier l'existence d'erreurs de période, au niveau de la comptabilisation de la facturation et de la livraison,
- vérifier l'existence d'erreurs de saisie dans le logiciel comptable à partir des données du tableur.

C. Opinion sur les comptes

Les travaux effectués n'ont pas relevé de points pouvant avoir une incidence sur l'opinion. Toutefois, les faiblesses relevées concernant les procédures de contrôle interne doivent faire l'objet d'une communication aux dirigeants.

D. Communication au gouvernement d'entreprise

Les recommandations suivantes sont adressées au gouvernement d'entreprise :

- L'embauche d'un nouveau directeur informatique est à réaliser rapidement. Le départ de l'ancien directeur informatique a entraîné une perte de la connaissance et de la maîtrise des processus informatiques de la société. M. Aloé, par manque de temps et de connaissances techniques, ne peut plus assurer la fonction de responsable informatique. Une perte de la maîtrise des systèmes d'information peut entraîner des dysfonctionnements et un manque de fiabilité des données traitées.

- Le nouveau directeur informatique devra mettre en place un schéma directeur afin de garantir dans le temps la cohérence du système d'information dans son ensemble et son adéquation aux besoins réels de la société.

- Siban est trop dépendante de la société de maintenance Indigo. Ceci représente un risque car, Indigo est propriétaire des codes sources et a la connaissance de toutes les applications utilisées par Siban. Elle est également en charge des développements et des évolutions des applications. En cas de désaccord avec la société ou de disparition de celle-ci, Siban pourrait se retrouver dans l'incapacité de gérer les dysfonctionnements de ces applications.

- Le système d'information utilisé à l'heure actuelle n'est plus adapté au volume de données à traiter (lenteur des traitements et pannes survenant fréquemment) : dans un premier temps, la société doit mettre en place une politique d'archivage des données afin de réduire le volume des données stockées, puis envisager un changement progressif des applications et matériels utilisés adaptés à de plus gros volumes de données. Les anomalies détectées peuvent entraîner des indisponibilités plus ou moins longues du système. Une indisponibilité du système d'information handicaperait grandement l'activité et les processus vitaux de la société, que ce soit au niveau des ventes via Internet, de la gestion des stocks, des commandes clients et fournisseurs ou des livraisons. En cas d'indisponibilité longue, des difficultés dans l'exploitation pourraient survenir.

- Concernant le projet de migration informatique, un état d'avancement et un suivi des coûts engagés et restant à engager sont à mettre en place. Ceci permettrait de chiffrer les frais que le projet devrait occasionner dans les exercices à venir. Selon les montants budgétés pour les exercices à venir, la constitution de provisions peut être envisagée.

- En termes de séparation des fonctions, il peut être préférable de former plusieurs personnes à la fonction exploitation ou d'identifier plusieurs personnes capables de seconder le responsable informatique dans ses fonctions. Ceci permettrait d'éviter que la gestion informatique ne soit affectée par le départ d'un responsable unique comme ce fut le cas lors du départ du directeur informatique.

- La sécurité logique et physique du système d'information est à améliorer : la politique des mots de passe et des habilitations est insuffisante à l'heure actuelle : la gestion des habilitations doit être suivie régulièrement (désactiver au plus vite le mot de passe de M.

Ginseng), le personnel doit être sensibilisé aux problèmes de sécurité et l'antivirus mis à jour régulièrement.

Les risques identifiés doivent conduire la société Siban à renforcer la qualité de son contrôle interne sur ces différents points. Pour ce faire, la société Siban devrait mettre en place les recommandations suivantes :

- procéder à la revue systématique des états d'anomalie générés par le système,
- définir une politique de gestion des droits d'accès conforme à l'organisation de la société,
- automatiser la génération de la facture après validation du bon de livraison, ou définir une procédure manuelle permettant de s'assurer qu'aucune livraison n'est effectuée sans envoi de la facture,
- définir une procédure permettant de s'assurer que les factures enregistrées avant la clôture concernent bien la période comptable concernée,
- mettre en place une interface automatisée entre Phytoventes et Phytocompta,
- réaliser une étude visant à assurer la conformité aux obligations fiscales en matière de comptabilité informatisée,
- déclarer à la CNIL l'ensemble des fichiers contenant des données nominatives.

3. GLOSSAIRE

Un grand nombre des définitions proposées provient du site Internet : www.dicofr.com.

Adresse IP

(Anglais : Internet Protocol)
Numéro constitué de quatre nombres entiers séparés par des points, qui identifie de façon unique un ordinateur connecté au réseau Internet et en permet la localisation (exemple : 213.38.15.23).

ADSL

(Anglais : Asymmetrical Digital Subscriber Line).
(Français : Ligne asymétrique numérique)
Technologie permettant le transport de plusieurs mégabits par seconde par ligne téléphonique.

Application

Les applications sont les logiciels à partir desquels sont effectués les traitements (traitements de texte, tableurs, navigateurs Internet).

Architecture

Terme général désignant la structure technique ou fonctionnelle de tout ou partie d'un système informatique.

Architecture client-serveur

Architecture composée d'un serveur gérant les bases de données communes et de plusieurs clients, permettant la distribution des applications.

ASP

1. (Anglais : Active Server Page)
Technologie Microsoft de création dynamique de pages Web.

2. (Anglais : Application Service Provider).
Méthode de commercialisation et technique consistant à louer sur un serveur une application logicielle (en Français, FAH, Fournisseur d'Application Hébergée).

Base de données

(Anglais : data base)
Fichier ou ensemble de fichiers permettant le stockage permanent ou temporaire et l'accès à des informations structurées.

Batch

Cf. Traitement par lot

Client

Application, installée sur le poste de l'utilisateur, accédant à des données situées sur un serveur distant.

Client-Serveur

Cf. architecture client-serveur.

Commerce électronique / en ligne

Vente de marchandises et de services proposés au travers de sites ou de messages personnalisés.

Commutateur

(Anglais : switch)
Elément permettant la communication entre deux segments de réseaux locaux.

Connexion

Procédure permettant à un utilisateur de se mettre en relation avec un système informatique et, si nécessaire, de se faire reconnaître de celui-ci.
(Journal officiel du 10 octobre 1998 "Liste des termes, expressions et définitions du vocabulaire de l'informatique")

CRM

(Anglais : Customer Relationship Management)
Logiciel de relation clientèle qui permet d'optimiser les relations entre une entreprise et ses clients.

Data mining

(Exploitation des données)
Analyse des données client collectées par l'entreprise à des fins commerciales.

DMZ

(Anglais : DeMilitarized Zone)
(Français : Zone DéMilitarisée)
Sous-réseau situé entre le réseau local et l'extérieur (Internet généralement). Contrôlée par un firewall, c'est la partie accessible de l'extérieur du réseau. Cette zone peut contenir les serveurs web, de messagerie, de news, proxy, ...

Données

(Anglais : Data)
Informations utilisées par un logiciel. Elles peuvent être créées par l'utilisateur ou par le programme lui-même.

Drill down

(Anglais : Data)
Mécanisme d'exploration des données caractérisant les outils de data mining. Il permet, à partir de la présentation d'une donnée synthétique, d'obtenir le détail de cette donnée.

E-business

La typologie des sites eBusiness (B = Business / C = Consommateur / A = Administration) :

B2C :	Sites s'adressant au grand public (ex : achat de biens culturels)
B2E :	Sites institutionnels s'adressant aux employés d'une entreprise (= intranet)
B2B :	Sites s'adressant aux entreprises (ex : places de marché virtuelles)
B2A :	Sites mettant en relation entreprises et administrations (ex : télédéclarations de TVA)
C2C :	Sites mettant en relation des particuliers (ex : vente aux enchères)

C2B : Sites mettant en relation des particuliers avec une entreprise (ex : achat groupé)
C2A : Sites mettant en relation particuliers et administrations (ex : télédéclarations d'impôts)

Les acteurs de l'eBusiness :

Clicks and surf (dotcoms) : sociétés présentes uniquement sur Internet
Clicks and mortar : sociétés traditionnelles présentes sur Internet
Bricks and mortar : sociétés traditionnelles absentes sur Internet

E-commerce

Cf. commerce électronique / en ligne

EDI

(Français : Echange de Données Informatisé ; Anglais : Electronic Data Interchange).
Transfert, entre systèmes d'information, de données structurées directement émises et traitées par des applications informatiques, selon des procédures normalisées.

E-mail

(Anglais : Electronic Mail).
(Français : message électronique, courriel, Mél)
Courrier électronique transmis par Internet, inventé en 1971.
Le signe @ est utilisé pour définir la machine à laquelle le message s'adresse.

ERP

(Anglais : Enterprise Resource Planning)
Logiciel de gestion d'entreprise, PGI en français.
Logiciel qui permet de gérer l'ensemble des processus d'une entreprise, en intégrant l'ensemble des fonctions de cette dernière comme la gestion des ressources humaines, la gestion comptable et financière, l'aide à la décision, mais aussi la vente, la distribution, l'approvisionnement et le commerce électronique.

Extranet

Réseau de télécommunication et de téléinformatique constitué d'un intranet étendu pour permettre la communication avec certains organismes extérieurs, par exemple des clients ou des fournisseurs.
(Journal officiel du 16 mars 1999 « Vocabulaire de l'informatique et de l'internet »).
Partie d'un intranet accessible à l'extérieur de l'entreprise à des personnes précises (login et mot de passe pour des clients par exemple) sur Internet.

FAI

Fournisseurs d'accès à Internet (Anglais : Provider).

Fichier

(Anglais : File)
Ensemble cohérent d'instructions ou de données au format numérique.

Fichier Log

Fichier contenant les informations de connexion et opérations des utilisateurs ou les anomalies résultant d'un traitement.

Firewall

Cf. Pare-feu

FTP

(Anglais : File Transfer Protocol).
Protocole Internet par lequel on peut envoyer (upload) ou recevoir (download) des fichiers.

GRC

Cf. CRM

Habilitation

Ensemble des droits d'accès d'un utilisateur, relatif à des données ou des programmes spécifiques.

Hosts (fichiers hosts)

Ordinateur distant qui reçoit les appels d'autres machines (connexions sur un site web par exemple).

HTML

(Anglais : HyperText Mark-up Language).
Langage de description des pages Web dérivé du SGML. Il est composé d'une suite de signes ASCII, dans laquelle sont inclues les commandes spéciales concernant le formatage des pages, la police de caractères et les éléments multimédia.

HTTP

(Anglais : HyperText Transfer Protocol).
Protocole utilisé pour transporter des pages HTML d'un site sur le réseau.
L'accès aux services Web se fait en donnant une adresse de type http://nom de domaine/répertoire...

Hypertexte

Système de renvois permettant de passer directement d'une partie d'un document à une autre, ou d'un document à d'autres documents (journal officiel du 16 mars 1999 « Vocabulaire de l'informatique et de l'internet »).

IHM

(Français : Interface Homme Machine)
Cf. Interface utilisateur.

Interface

Programme permettant un échange de données entre des applications différentes.

Interface utilisateur

Partie visible par l'utilisateur d'un logiciel,
le programme gérant l'interaction entre la machine et l'utilisateur.

Internet

Réseau informatique mondial constitué d'un ensemble de réseaux nationaux, régionaux et privés, qui sont reliés par le protocole de communication TCP-IP et qui coopèrent dans le but d'offrir une interface unique à leurs utilisateurs.

Internet Protocol

(Abréviation : IP)
Cf. adresse IP.

Intranet

Réseau de télécommunication et de téléinformatique destiné à l'usage exclusif d'un organisme et utilisant les mêmes protocoles et techniques que l'Internet.
(Journal officiel du 16 mars 1999 « Vocabulaire de l'informatique et de l'internet »)

Langage

Ensemble des caractères, des symboles, des mot-clés et des règles permettant de les assembler, utilisé pour donner des instructions à un ordinateur.

Log

Cf. Fichier log.

Logiciel

(Anglais : Software)
Cf. application.

Login

Procédure de connexion à une application.

Logout

Procédure de déconnexion à une application.

Navigateur

(Anglais : Browser)
Dans un environnement de type Internet, logiciel qui permet à l'utilisateur de rechercher et de consulter des documents, et d'exploiter les liens hypertextuels qu'ils comportent.
(Journal officiel du 16 mars 1999 « Vocabulaire de l'informatique et de l'internet »)

Nœud (de réseau)

Unité connectée à un réseau (un serveur, un poste de travail, un routeur, une imprimante peuvent constituer un nœud de réseau).

Paramètre

Variable intervenant dans l'exécution d'un programme.

Pare-feu

(Anglais : Firewall)
Dispositif informatique qui filtre les flux d'informations entre un réseau interne à un organisme et un réseau externe en

vue de neutraliser les tentatives de pénétration en provenance de l'extérieur et de maîtriser les accès vers l'extérieur.
(Journal officiel du 16 mars 1999 « Vocabulaire de l'informatique et de l'internet »)

Périphérique

Matériel distinct de l'unité centrale de traitement (microprocesseur) à laquelle il est relié et qui peut assurer l'entrée ou la sortie de données.

PGI

Cf. ERP

POP

Protocole de courrier électronique : les logiciels de messagerie utilisent ce protocole et service TCP/IP "bureau de poste", pour récupérer le courrier électronique de l'utilisateur auprès du FAI.

Portail

Cf. Site portail

Progiciel

(Français : PROduit loGICIEL)
Logiciel professionnel standard par opposition aux logiciels développés spécifiquement pour les besoins d'une entreprise.

Port

(Réseaux)
Lors d'une connexion à un ordinateur hôte, il est nécessaire de spécifier l'adresse de cet hôte mais aussi son port. Le numéro de port va spécifier le type de communication avec l'hôte. Par exemple, le port pour une communication Telnet est 23, celle pour une communication HTTP est 80... Le choix du port est aujourd'hui dans la plupart des cas automatique.

Processus

« Enchaînement de tâches, manuelles, semi-automatiques, automatiques, concourant à l'élaboration, à la production ou au traitement d'informations, de produits ou de services. Exemples : processus de gestion des ventes, processus de gestion des impayés, processus de fabrication, processus d'inventaire permanent, processus d'établissement des comptes, etc.». (Comité d'application des normes professionnelles de la CNCC – septembre 2002).

Programme d'application

Cf. Application.

Protocole

(Anglais : Protocol).
Description des formats de messages et règles selon lesquelles deux ordinateurs échangeront des données. Les protocoles décrivent également les détails de bas niveau sur la façon dont deux machines communiquent ou des échanges de haut niveau entre deux programmes.

Référentiel

(Anglais : repository.)
Ensemble structuré d'informations, utilisé pour l'exécution d'un logiciel, et constituant un cadre commun à plusieurs applications.
(Journal officiel du 10 octobre 1998 « Liste des termes, expressions et définitions du vocabulaire de l'informatique »)

Réseau

(Anglais : Network)
Un réseau informatique peut être local ou élargi (réseau longue distance). Il permet la transmission de tout type de données, échangées sous forme numérique et exploitables par l'ensemble du système relié en réseau.

Routeur

(Anglais : router).
Outil logiciel ou matériel pour diriger les données à travers un réseau. Il s'agit souvent d'une passerelle entre plusieurs serveurs pour que les utilisateurs accèdent facilement à toutes les ressources proposées sur le réseau. Le routeur désigne également une interface entre deux réseaux utilisant des protocoles différents.

Serveur

(Anglais : server, on-line data service.)
Système informatique destiné à fournir des services à des utilisateurs connectés et, par extension, organisme qui exploite un tel système.
Note : un serveur peut par exemple permettre la consultation et l'exploitation directe de banques de données.
(Journal officiel du 16 mars 1999 « Vocabulaire de l'informatique et de l'internet »)

Serveur d'applications

Serveur hébergeant les applications auxquelles accèdent à distance les utilisateurs habilités.

SGBD

(Français : Système de Gestion de Bases de Données)
(Anglais : Data Base Management System, DBMS).
Logiciel permettant de stocker les données, de les mettre à jour et de les consulter.

Site Portail

Terme générique pour désigner un site qui sert de point d'entrée sur Internet à d'autres sites liés les uns aux autres.

SMTP

(Anglais : Simple Mail Transfer Protocol).
Dans un réseau TCP/IP, ce protocole gère l'envoi de mails entre différents serveurs. Il est également utilisé pour l'envoi de mails à partir des ordinateurs clients. C'est pour cette raison que doivent être spécifiés un serveur POP et un serveur SMTP dans la configuration des logiciels de mails.

SPAM

Envoi massif et parfois répété, de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'Internet : forum de discussion, listes de diffusion, annuaires, sites web, etc. (Définition CNIL)

Structure de fichier

Représentation conceptuelle des relations entre la valeur des données, les enregistrements et les fichiers. La structure décrit en général la manière dont les données sont stockées et comment elles doivent être manipulées.

Suite logicielle

Ensemble (package) de modules/programmes intégrés dans le cadre d'une application (bureautique, communication, etc.)

Système d'exploitation

(Anglais : Operating System)
Programme assurant la gestion de l'ordinateur et de ses périphériques.

Switch

Cf. commutateur

TCP/IP

(Anglais : Transmission Control Protocol/Internet Protocol)
Ensemble de protocoles standards permettant la communication dans un environnement hétérogène. Protocole de la couche Transport, il fournit un protocole de gestion de réseau d'entreprise routable ainsi que l'accès à Internet. Il comporte également des protocoles de la couche Session. Pour être en mesure d'échanger des données entre différents ordinateurs, TCP/IP exige de spécifier les trois valeurs suivantes : une adresse IP, un masque de sous-réseau et une passerelle (routeur) par défaut.

Temps réel

Traitement informatique effectué au moment où est lancée la requête ou transaction.

Temps différé

Traitement informatique déconnecté du lancement de la requête ou de la transaction (en général, la nuit ou en fin de semaine). Sont essentiellement concernés les traitements nécessitant une ressource machine importante, qui ralentiraient trop fortement le système dans son ensemble s'ils étaient lancés pendant la journée.

Traitement par lots

(Anglais : batch processing).
Mode de traitement des données suivant lequel les programmes à exécuter ou les données à traiter sont groupés en lots.

Virus

Programme hostile susceptible d'infecter les fichiers (principalement les fichiers exécutables) en y insérant une copie de lui-même. Il peut en résulter des

dysfonctionnements divers, effacement du disque dur, etc.

VPN

(Anglais : Virtual Private Network)
Définit un réseau privé virtuel sur un réseau public (tel Internet).

4. BIBLIOGRAPHIE

4.1. Ouvrages management et NTIC

- CHOWDHURY Subir, « Management 21C », Financial Times, Prentice Hall, A Pearson Education Book, 2002, 289 pages.
- ETTIGHOFFER Denis, « L'entreprise virtuelle : nouveaux modes de travail, nouveaux modes de vie ? », Editions d'Organisation, 2001, 392 pages.
- BOCHURBERG Lionel, « Internet et commerce électronique », Delmas, 2001, 352 pages.

4.2. Ouvrages d'audit

- Compagnie nationale des commissaires aux comptes (CNCC) : « La démarche du commissaire aux comptes en milieu informatisé », CNCC Edition, 1995, 142 pages.
- CHARRON Claude : « Normes internationales d'audit : International Federation of Accountants (IFAC) handbook 1998 : traduction française », CNCC Edition, 1998, 524 pages.
- Information Systems Audit and Control Association (ISACA) : « COBIT : gouvernance, contrôle et audit de l'information et des technologies associées », Association Française de l'Audit et du Conseil Informatiques (AFAI), 2000, 485 pages.
- Information Systems Audit and Control Foundation (ISACA) : « Digital Signatures, Sécurity & Controls », 1999, 156 pages.
- Association Française de l'Audit et du Conseil Informatiques (AFAI), « CIME, Conduite Informatique des Moyennes Entreprises », 2002, 127 pages.
- Institut Français des Auditeurs Internes (IFACI) : « Audit et contrôle des systèmes d'information : traduction française du SAC Report », IFACI, 1993, X volumes.
- International Federation of Accountants (IFAC) : « International Information Technology Guideline 1 : Managing security of information », IFAC (www.ifac.org/store), 1998, 19 pages.
- The Canadian Institute of Chartered Accountants (ICCA) : « Strategic Internet Commerce », 1999, 165 pages.

4.3. Ouvrage technique

- Techniques de l'ingénieur : « Technologies de l'Internet », édition n° 2, CD-ROM.

4.4. Ouvrages juridiques

- BOCHURBERG Lionel, « Internet et commerce électronique », Delmas, 2001, 352 pages.
- FERAL-SCHUL Christiane, « Cyberdroit », Dalloz Dunod, 2002, 353 pages.
- BILON Jean-Louis, « Fiscalité du numérique », Litec, 2000, 213 pages.
- FENOLL-TROUSSEAU Marie-Pierre et HAAS Gérard, « Internet et protection des données personnelles », Litec, 2000, 206 pages.

4.5. Articles

4.5.1. Informatique

- C.L.P, « Comment ça marche un antivirus… ? », IT-Expert n° 37, mai/juin 2002.
- Dossier sécurité, IT-Expert n° 39, septembre/octobre 2002.
- « Services web : la sécurité en marche », Décision micro et réseaux n° 525, semaine du 28 octobre au 3 novembre 2002.
- « La sécurité au centre de l'entreprise en réseaux », La Tribune, Le cahier informatique, n° 2527, mardi 5 novembre 2002.

4.5.2. Protection des droits de propriété intellectuelle

- ARCHAMBAULT Jean-Pierre, (2001 septembre) « Logiciel et propriété intellectuelle » sur le site La revue de l'EPI. Page consultée le 18/10/2002. (http://www.epi.asso.fr/revue/103/ba3p065.htm)
- CAHEN Murielle, (sans date) « Interdiction de copier : freeware, shareware et careware » sur le site Marketing-Internet. Page consultée le 17/10/2002. (http://marketing-internet.com/articles/juridique/copier.html)
- Le forum des droits sur l'internet, (2001, 29 novembre) « Créer un site Web », sur le site Forum des droits de l'Internet (http://www.foruminternet.org/documents/en_pratique/lire.phtml?id=211)

4.5.3. Respect de la vie privée et protection des données personnelles

- CAHEN Murielle, (2002, 20 février) « Les aspects juridiques du spamming » sur le site Clic Droit (http://www.clic-droit.com)
- POULLET Yves, (2001, 17 février) « Internet et Vie privée : entre risques et espoirs » Le Journal des Tribunaux n° 6000. Page consultée le 18 septembre 2002. (http://www.unitar.org/isd1/dt/vie-priv-poullet.pdf)

- STAUB Sylvain, (2002, 8 octobre) « Spam : ce que va changer la directive du 12 juillet » sur le site Journal du Net. Page consultée le 18 septembre 2002. (http://www.journaldunet.com/juridique/juridique021008.shtml)

- Sans auteur, (2002, 16 juillet) « Maîtriser son identité sur l'Internet », sur le site Forum des Droits de l'Internet. Page consultée le 17 septembre 2002. (http://www.foruminternet.org/documents/en_pratique/lire.phtml?id=301)

4.5.4. Pratiques commerciales

- THOUMYRE Lionel, (1999) « L'échange des consentements dans le commerce électronique », Lex Electronica. Page consultée le 16 octobre 2002. (http://www.lex-electronica.org/articles/v5-1/thoumfr.htm)

- VERBIEST Thibault, (2001, 4 Septembre) « Commerce électronique : la France transpose la directive sur les contrats à distance » sur le site Droit Nouvelles Technologies. Page consultée le 17 septembre 2002. (http://www.droit-technologie.org/1_2.asp?actu_id=460)

4.5.5. Fiscalité

- BOULIN François-Xavier, (2002, 8 mai) « Le Conseil adopte le nouveau régime de TVA applicable aux services fournis par voie électronique » sur le site Droit-NTIC.com. Page consultée le 18/10/2002. (http://www.droit-ntic.com/MyNews1.2/ read_comment.php3?id)

- VERBIEST Thibault, (sans date) « Les nouvelles règles de la TVA appliquée au commerce électronique » sur le site Journal du Net. Page consultée le 17/10/2002. (http://www.journaldunet.com/juridique/juridique020626.shtml)

- C.VERGES Alexandra, (1997, 18 février) « Commerce électronique : une fiscalité à inventer » Les Echos. Page consultée le 18/10/2002. (http://www.acv-taxlaw.com/commerce_electronique_echos.htm)

- WOODSIDE Simon, (2001, 05 février) « La fiscalité du commerce électronique : Une réalité virtuelle » OCDE L'observateur. Page consultée le 17/10/2002. (http://www.observateurocde.org/news/fullstory.php/aid/391/La_fiscalité_du_commerce_électronique_:_Une_réalité_virtuelle.html)

4.6. Annuaires et portails

- Juriguide : http://www.juriguide.com/pages/index.html

- Juridiconline : http://www.juridiconline.com/

- Dicofr (dictionnaire de l'informatique) : www.dicofr.com

4.6.1. Sites généralistes du droit des nouvelles technologies

- Droit-ntic : Information et de réflexion sur les implications juridiques des nouvelles technologies de l'information et de la communication. (http://droit-ntic.com/)

- Forum des droits sur l'Internet : Espace d'information et de débat sur les questions de droit et de société de l'Internet et des réseaux. (http://www.foruminternet.org)

- Juriscom.net : Actualités, articles, lois, jurisprudence, relatifs au droit des nouvelles technologies. (http://www.juriscom.net/)

- Le Club.sénat.fr : Réflexions et propositions concrètes sur des thèmes relatifs à la nouvelle économie (http://club.senat.fr/)

- 01net : Journal des nouvelles technologies envisagées sous les angles pratiques et juridiques. (http://www.01net.com/)

4.6.2. Sites et annuaires spécialisés

A. Protection des droits de propriété intellectuelle

- Legalbiznet : actualité juridique de la propriété intellectuelle intéressant les nouvelles technologies (brevet, logiciel, droit d'auteur, marque, contrefaçon, noms de domaines…) (http://www.legalbiznext.com/)

- Revue Internationale du Droit d'Auteur : la version électronique de la revue papier du même nom propose son sommaire en ligne ainsi qu'un résumé de chaque article de doctrine qui paraît dans la revue. (http://www.la-rida.com/)

- Organisation Mondiale de la Propriété Intellectuelle : actualité, information, activité et services, questions nouvelles en matière de propriété intellectuelle. (http://www.ompi.org/index.html.fr)

- SACEM : Société des auteurs compositeurs et éditeurs de musique. (http://www.sacem.fr)

- Saceml : un site et un groupe de discussion et d'information à propos de l'aspect juridique, légal et statutaire du droit d'auteur de la musique en France. (http://saceml.deepsound.net/)

- IRPI : Institut de recherche en propriété intellectuelle (http://www.ccip.fr)

- ADAGP : Société des auteurs dans les arts graphiques et plastiques (http://www.adagp.fr)

- SACD : Société des auteurs et compositeurs dramatiques (http://www.sacd.fr)

- SCAM : Société civile des auteurs multimédia (http://www.scam.fr)

- SESAM : Société de gestion des droits (http://www.sesam.org)

B. Vie privée et données personnelles

- CNIL : La Commission Nationale Informatique et Liberté est l'organe chargé de veiller au respect de la loi française sur la protection de la vie privée. Son site présente les textes officiels, des dossiers thématiques, une synthèse des droit et obligations. (http://www.cnil.fr/)

- OCDE : l'OCDE, organisme international, met à disposition du public un outil qui permet de générer à la seconde, et gratuitement, une charte vie privée destinée aux sites web. (http://cs3-hq.oecd.org/scripts/pwv3/pwhome.htm)

- Iris : site d'une association française qui a pour ambition d'agir sur le développement de l'Internet vers plus d'égalité, et de solidarité. Il présente des dossiers sur la responsabilité des fournisseurs, les contenus libres, la cryptographie, etc. (http://www.iris.sgdg.org/)

C. Commerce électronique

- Mission pour l'économie numérique : les objectifs de la mission commerce électronique du Ministère de l'Economie, des Finances et de l'Industrie sont notamment d'impulser une réflexion prospective sur des sujets tels que le commerce électronique, la sécurité, la signature électronique, la monnaie numérique, la dématérialisation des marchés publics, la fiscalité ou les jeux en ligne. Les rapports des groupes de travail sont en ligne sur le site. (http://www.men.minefi.gouv.fr/)

- CNUDCI : Commission de l'ONU pour le droit commercial international : la commission spécialisée de l'ONU en charge du commerce international propose en ligne des lois types, les conventions internationales, et un recueil de jurisprudence mondiale ayant appliqué ou interprété les textes de la CNUDCI. (http://www.uncitral.org/)

- Club de la Sécurité des Systèmes d'Information Français (CLUSIF) : dossier an 2000, textes sur la cryptologie, dossier sur l'évaluation des conséquences économiques des incidents dus à l'informatique… (https://www.clusif.asso.fr)

- Cybercommerce : Ministère des finances. (http://www.finances.gouv.fr)

D. Fiscalité

- Fiscal on line : site de droit fiscal généraliste et e-fiscalité.(http://www.fiscalonline.com/)

E. Management

- Business minds : librairie d'ouvrages en management. (www.business-minds.com)